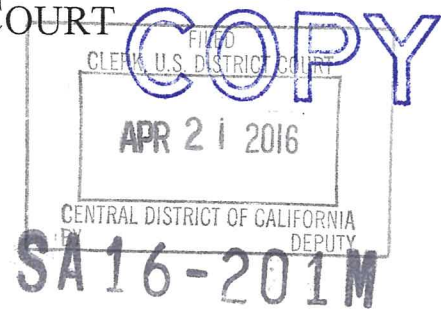


UNITED STATES DISTRICT COURT

for the
Central District of California



In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

A silver-colored laptop, HP model Notebook, located on the
floor in the sole bedroom of SUBJECT PREMISES #1,
marked by agents as Digital Device #54

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-5

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, United States Code, Sections 286, 287, 371, 1001, 1028
(a)(7), 1343, 1344, and 1956

Offense Description

See attached Affidavit

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

LODGED

2016 APR 21 AM 11:32
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
SANTA ANA

Sworn to before me and signed in my presence.

Date: 4-21-16

City and state: Los Angeles, CA

Applicant's signature

IRS-CI SA LEIA BELLIS

Printed name and title

Judge's signature

U.S. Magistrate Judge

Printed name and title

KAREN E. SCOTT

A F F I D A V I T

I, Leia Bellis, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Internal Revenue Service - Criminal Investigation ("IRS-CI"), assigned to the Los Angeles Field Office, and have served in this capacity since July 2015. I have been a Special Agent since August 2002. I received a Bachelor of Science degree in Psychology from San Diego State University in May 2002. My duties and responsibilities include the investigation of possible criminal violations of the Internal Revenue laws (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), the Money Laundering Control Act of 1986 (Title 18, United States Code, Sections 1956 and 1957), and other related offenses. I attended the Criminal Investigator Training Program and the IRS SA Basic Training at the Federal Law Enforcement Training Center, where I received detailed training in conducting financial investigations. My training included courses in law enforcement techniques, federal criminal statutes, criminal investigations, execution of search warrants, financial investigative techniques, and legal principles and statutes representing criminal violations of Titles 18, 26, and 31 of the United States Code.

2. I have conducted and assisted in investigations involving financial crimes. I have led and participated in

[Instrumentality Protocol]

search warrants and have interviewed witnesses and defendants who were involved in, or had knowledge of, violations of the Internal Revenue Code, the Bank Secrecy Act, and the Money Laundering Control Act. In the course of my employment with IRS-CI, I have conducted or been involved in investigations of alleged criminal violations, which have included tax evasion (26 U.S.C. § 7201), filing a false tax return (26 U.S.C. § 7206(1)), aiding or assisting in the preparation of false tax returns (26 U.S.C. § 7206(2)), conspiring to defraud the United States (18 U.S.C. § 371), wire and mail fraud (18 U.S.C. §§ 1343 and 1341), aggravated identity theft (18 U.S.C. § 1028A), and money laundering (18 U.S.C. §§ 1956 and 1957), among others. I have also led and participated in the execution of federal search warrants and the consensual searches of records involving the seizure of records relating to the concealment of assets and proceeds derived from fraud. These records included, but were not limited to, telephone bills, personal telephone books, emails, photographs, records pertaining to the purchase of real property, bank records, escrow records, credit card records, tax returns, business books and records, and computer hardware and software.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for warrants to search for evidence of violations of Title 18, United States Code, Sections 286, 287, 371, 1001, 1028(a)(7),

1343, 1344, and 1956, which criminalize, respectively, conspiracy to defraud the United States with respect to claims, false claims, conspiracy to defraud the United States, making or using false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry, identity theft, wire fraud, bank fraud, and money laundering.

4. The digital devices to be searched are:

a. A black-colored laptop, Dell model Latitude, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #32 (SUBJECT LAPTOP #1), as more fully described in Attachment A-1;

b. A silver-colored laptop, Lenovo model Ideapad 100S, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #29 (SUBJECT LAPTOP #2), as more fully described in Attachment A-2;

c. A black-colored laptop, Toshiba model Satellite, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #30 (SUBJECT LAPTOP #3), as more fully described in Attachment A-3;

d. A blue-colored laptop, HP model Stream, located on the floor in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #59 (SUBJECT LAPTOP #4), as more fully described in Attachment A-4;

e. A silver-colored laptop, HP model Notebook, located on the floor in the sole bedroom of SUBJECT PREMISES #1,

marked by agents as Digital Device #54 (SUBJECT LAPTOP #5), as more fully described in Attachment A-5;

f. A black-colored laptop, Dell, located on the floor in the sole bedroom of SUBJECT PREMISES #1, on top of a printer, marked by agents as Digital Device #55 (SUBJECT LAPTOP #6), as more fully described in Attachment A-6;

g. A black-colored laptop, Toshiba model Satellite, located on a shelf in the closet in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #60 (SUBJECT LAPTOP #7), as more fully described in Attachment A-7;

h. A black-colored laptop, Toshiba model Satellite, located with SUBJECT LAPTOP #7 on a shelf in the closet in the sole bedroom of subject of SUBJECT PREMISES #1, marked by agents as Digital Device #61 (SUBJECT LAPTOP #8), as more fully described in Attachment A-8;

i. A black-colored laptop, Lenovo model Ideapad 100, located on a folding table near the front door of SUBJECT PREMISES #1, marked by agents as Digital Device #1 (SUBJECT LAPTOP #9), as more fully described in Attachment A-9;

j. A black-colored laptop, Dell, located on a folding table near the front door of SUBJECT PREMISES #1 with SUBJECT LAPTOP #9, marked by agents as Digital Device #2 (SUBJECT LAPTOP #10), as more fully described in Attachment A-10;

k. A black-colored laptop, HP model Notebook, located on a bookshelf in the main room of SUBJECT PREMISES #1, inside a box, marked by agents as Digital Device #3 (SUBJECT LAPTOP #11), as more fully described in Attachment A-11; and

l. A black Ipad, with a silver back, located on the desk near SUBJECT LAPTOP #1 under some papers, marked by agents as Digital Device #53 (SUBJECT IPAD #1), as more fully described in Attachment A-12 (collectively, the "SUBJECT DEVICES"). The requested search warrants seek authorization to seize any data on the SUBJECT DEVICES that constitutes evidence or fruits of violations of Title 18, United States Code, Sections 286, 287, 371, 1001, 1028(a)(7), 1343, 1344, and 1956 (collectively, the "Subject Offenses"), or any SUBJECT DEVICE that is itself an instrumentality of the Subject Offenses.

5. The SUBJECT DEVICES are identified in Attachments A-1 to A-12 to the search warrant application. The list of items to be seized is set forth in Attachment B to the search warrant application. Attachments A-1 to A-12 and B are incorporated herein by reference.

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants and does not purport to set forth all of my knowledge of or

investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. STATEMENT OF PROBABLE CAUSE

A. Summary of Investigation

7. IRS-CI and the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), have been investigating a large fraud ring that has been laundering tens of millions of dollars in tax refunds that were fraudulently obtained from false federal tax returns that had been filed using stolen identities.

B. April 20, 2015, Search Warrants Executed

8. On April 19, 2015, the Honorable Karen E. Scott, United States Magistrate Judge, authorized a federal search warrant for SUBJECT PREMISES #1, 10987 Bluffside Drive, Unit 4209, Studio City, California 91604 (see Attachment C: Search Warrant SA 16-174M), which I incorporate by reference into this Affidavit.

9. On April 20, 2015, IRS-CI, HSI, and FBI agents executed the above-referenced search warrant on SUBJECT PREMISES #1.

10. On April 20, 2015, I spoke with SA Adrian Yopez, who is one of the lead case agents in the investigation involving

SUBJECT PREMISES #1, and other SAs, who took part in the execution of the above-referenced search warrant of SUBJECT PREMISES #1, and learned the following:

a. At approximately 11:30 a.m., SCHEMER#12 entered SUBJECT PREMISES #1 carrying a large box that appeared to be a moving box.

b. Throughout the day, SCHEMER#8, SCHEMER#9, SCHEMER#12, SCHEMER#15, and Unidentified Female #1 were observed talking on the balcony of SUBJECT PREMISES #1.

c. At approximately 12:30 p.m., SCHEMER#1 arrived to SUBJECT PREMISES #2. Agents observed SCHEMER#1 using multiple different cellular telephones to make multiple calls.

d. At approximately 4:00 p.m., SCHEMER#1 left SUBJECT PREMISES #2, and agents followed SCHEMER#1 to the Avalon Apartments complex.

e. At approximately 4:15 p.m., SCHEMER#1 entered SUBJECT PREMISES #1.

f. At approximately 4:20 p.m., agents executed the search warrant for SUBJECT PREMISES #1, and entered SUBJECT PREMISES #1.

g. When agents entered SUBJECT PREMISES #1, SCHEMER#1, SCHEMER#8, SCHEMER#13, SCHEMER#15, and Unidentified Female #1 were inside SUBJECT PREMISES #1.

h. SA Yepez observed the following inside the sole bedroom of SUBJECT PREMISES #1:

i. A desk that had three laptop computers on it, as depicted on Attachment D:

1. A black-colored laptop, Dell model Latitude, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #32 (SUBJECT LAPTOP #1);

2. A silver-colored laptop, Lenovo model Ideapad 100S, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #29 (SUBJECT LAPTOP #2);

3. A black-colored laptop, Toshiba model Satellite, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #30 (SUBJECT LAPTOP #3);

ii. Also on the desk were one Ipad (described below as SUBJECT IPAD #1), and 7 cell phones. Also on that desk was a red 3-hole binder with copies of many checkcards.

i. I also spoke with IRS-CI SA Jerome Jenkins, who told me that the following 8 laptops and one Ipad were also found inside SUBJECT PREMISES #1:

i. A blue-colored laptop, HP model Stream, located on the floor in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #59 (SUBJECT LAPTOP #4);

ii. A silver-colored laptop, HP model Notebook, located on the floor in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #54 (SUBJECT LAPTOP #5);

iii. A black-colored laptop, Dell, located on the floor in the sole bedroom of SUBJECT PREMISES #1, on top of a printer, marked by agents as Digital Device #55 (SUBJECT LAPTOP #6);

iv. A black-colored laptop, Toshiba model Satellite, located on a shelf in the closet in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #60 (SUBJECT LAPTOP #7);

v. A black-colored laptop, Toshiba model Satellite, located with SUBJECT LAPTOP #7 on a shelf in the closet in the sole bedroom of subject of SUBJECT PREMISES #1, marked by agents as Digital Device #61 (SUBJECT LAPTOP #8);

vi. A black-colored laptop, Lenovo model Ideapad 100, located on a folding table near the front door of SUBJECT PREMISES #1, marked by agents as Digital Device #1 (SUBJECT LAPTOP #9);

vii. A black-colored laptop, Dell, located on a folding table near the front door of SUBJECT PREMISES #1 with SUBJECT LAPTOP #9, marked by agents as Digital Device #2 (SUBJECT LAPTOP #10);

viii. A black-colored laptop, HP model Notebook, located on a bookshelf in the main room of SUBJECT PREMISES #1,

inside a box, marked by agents as Digital Device #3 (SUBJECT LAPTOP #11);

ix. A black Ipad, with a silver back, located on the desk near SUBJECT LAPTOP #1 under some papers, marked by agents as Digital Device #53 (SUBJECT IPAD #1).

j. Also on the desk was a document that appeared to be similar to a general ledger, i.e., it had columns entitled dates, amount, balance, date, name, bank, "acc", and amount.

k. SUBJECT LAPTOP #1 was powered on, and agents observed that on the screen was the logon screen for Bank of America.

l. Also located on the desk was a letter from a bank addressed to "Nugzar Arutinov," at 5404 Whitsett Ave. #179, Valley Village, California. Another letter from Synchrony Bank was also addressed to "Nugzar Arutinov" at the same address. For reference, "Nugzar Arutinov" was one of the identities used by SCHEMER#9, as described in the aforementioned Affidavit.

m. Throughout SUBJECT PREMISES #1, agents found a total of approximately 105 cellular phones (which includes the 7 phones found on the desk described above). Many of the cellular telephones had Stickers with names and/or phone numbers on them that are tied to identities used in the scheme.

i. For example, one of the telephones had a sticker with the telephone number of 818-298-6843 and the name "Tsalok Sozamyman" written on it. For reference, as described in

the aforementioned Affidavit, that is the name in which SUBJECT PREMISES #1 was rented, with false information.

ii. For example, another of the telephones had the name "Elina Oganessian" and the telephone number 626-720-9719 written on it. For reference, as described in the aforementioned Affidavit, that is the name of one of the identities used by SCHEMER#6.

iii. Also located were stamps with "pay to the order of BofA Woodland Hills, dba Nozimjan Style and Design, ANNAV Nozimjon Sole proprietor 325060492883."

iv. Agents also found a safe, which was opened using the key in it. Inside the safe, agents found cash and several passports. One of the passports was a Republic of Armenia passport in the name "Vahagn Vardanyan" with number AM0617861. For reference, that was one of the identities and passports used by SCHEMER#3 to open a mailbox.

v. Also with the desk was a booklet with multiple bankcards in many different names.

vi. During execution of the search warrant, SCHEMER#15 threw a purse over the balcony, which agents subsequently retrieved. That purse had inside of it multiple thumbdrives, a simcard, keys, and several notes with what appear to be names with account numbers, email addresses, a code number, and addresses.

11. On April 20, 2015, I spoke with SA Adrian Yepez, who is one of the lead case agents in the investigation involving SUBJECT PREMISES #1. Based on that conversation, I know the following:

a. This investigation has identified the use of computers in the filing of false returns, on-line banking activity, and the creation of email addresses that were used as identification in opening bank accounts. Based on my training and experience, and my conversation with SA Yepez, I know that the perpetrators of these types of schemes typically do not use static IP addresses or any IP address which would identify the perpetrator. Therefore a link between a particular IP address at one of the scheme locations and this fraud scheme would not be expected.

b. On May 18, 2015, U.S. Bank provided SA Yepez with a spreadsheet containing all of the IP addresses that had ever accessed the bank accounts opened in the name of "Artur Poghosyan," from February 27, 2014, to April 1, 2015. SA Yepez researched the IP addresses provided and identified their geological locations and their IP Providers. In doing so, SA Yepez discovered the following:

i. Verizon Wireless was the IP provider for all of the IP addresses he had researched.

ii. The geological locations for the IP addresses were within Los Angeles County, with the majority of the access locations being in the city of Los Angeles.

iii. The IP addresses that accessed the bank accounts in 2014 were static locations, meaning the IP address was assigned to a specific subscriber and location, whereas the IP addresses that accessed the bank accounts in 2015 were dynamic. A dynamic IP addressing assigns a different IP address each time the customer logs on to their computer.. One dynamic IP address is often assigned to different users, thus making it difficult to identify a specific user and computer.

iv. Review of the IP address records showed that multiple Device Identification Numbers ("Device ID") were used to access the bank accounts on-line. A Device ID is a distinctive number associated with a specific computer, hand held device, or phone. In addition to financial institutions, the IRS tracks all device IDs from computers and smartphones that are used to electronically transmit tax returns. Computers and digital devices found at the SUBJECT PREMISES #1 could contain the above mentioned evidence and Device IDs. That evidence is critical to the investigation in proving knowledge, intent, and identifying other victims and perpetrators.

v. In addition, SA Yepez told me that based on the investigation, and his training and experience, he believes that a computer is being used in the scheme to alter documents

and foreign passports used to open private mail boxes and bank accounts. For example, SA Yepez has reviewed 181 private mailbox files from several commercial mail receiving agencies located in Los Angeles and Orange Counties. The private mail box files often included an application to rent the private mail box, contract, Form 1583, foreign passport, utility bills, and/or insurance cards.

1. Utilities bills purportedly from Time Warner Cable were used at least 22 times, bills purportedly from AT&T were used at least 23 times, bills purportedly from Dish Network were used at least 3 times, and bills purportedly from T-Mobile were used at least 2 times.

2. Each bill purported to be from those companies displays the account holder's name, address, account number, a service period, and amount due. In some instances, the same account number was used multiple times.

3. On April 13, 2016, SA Yepez called Time Warner Cable representative, who explained to him that all Time Warner Cable bills for the western part of the United States, including states like California, Arizona, and Colorado have account numbers that begin with the numbers "8448." Of the 22 Time Warner Cable bills discussed above, 11 had an account number that did not begin with "8448." All of the Time Warner Cable bills that SA Yepez reviewed purported to be servicing addresses in California, so the ones with account numbers that

do not begin with 8448 appear to be altered. In fact, SA Yepez also found that the same account number was used on different Time Warner Cable bills. The chart below summarizes the utility bills provided by the schemers to open private mail boxes. Based on the information above, SA Yepez and I believe the schemers are using a computer to scan and alter utility bills and other documents.

TIME WARNER CABLE (22)	AT&T (23)	STATE FARM INSURANCE CARD (4)	DISH NETWORK (3)	UNITRIN INSURANCE CARD (2)	T-MOBILE (2)	CATAIC LAKE WATER AGENCY (1)	PACIFIC SPECIALTY INSURANCE (1)
Mikayel Abrahamayan	Khachatur Khachatryan	Gurgen Mutaftyan	Hamlet Muradyan	Garnik Keryan	Tehmine Khachatryan	Avetisyan Karen	Demetry Genzer
Gevorg Martirosyan	Robert Baghdasaryan	Kamo Khachatryan	Hyak Vardanyan	Boris Ghevondyan	Hakob Harutyunyan		
Mesrop Petrosyan	Ani Nahapetyan	Artak Serobyan	Sergey Gevorgyan				
Tigran Manukyan	Anahit Israelyan	Paylak Avetisyan					
Gagik Sahakyan	Andranik Ustiyen						
Sargis Shahbazyan	Vepkhia Beriandze						
Edgar Vardanyan	Sasha Grigoryan						
Mamikon Zeynalyan	Mkrtich Manukyan						
Iveta Mkrtchyan	Samvel Danielyan						
Elena Oganesyany	Hachik Arakelyan						
Mher Grigoryan	Vahram Nahapetyan						
Sargis Manukyan	Giorgo Gevorkian						
Edik Nasirov	Anush Karapetyan						
Nugzar Arutinyov	Tamara Andriasyan						
Vaghinak Sosyan	Gegham Mkhitarayan						
Davit Movsisyan	Hasanboy Ergashev						
Emzar Tsenteradze	Martun Shermazanyan						
Robert Hovhannisyan	Aram Vardanyan						
Hakob Harutyunyan	Narek Kocharyan						
Anzhela Hambardzumyan	Artur Gevorgyan						

TIME WARNER CABLE (22)	AT&T (23)	STATE FARM INSURANCE CARD (4)	DISH NETWORK (3)	UNITED INSURANCE CARD (2)	T-MOBILE (2)	CATAIC LAKE WATER AGENCY (1)	PACIFIC SPECIALTY INSURANCE (1)
Artur Poghosyan	Arman Saghatelyan						
Anna Vardazaryan	Khachik Avagyan						
	Armen Ionesyan						

12. During our conversation on April 20, 2015, SA also discussed SCHEMER#13, who was discussed in the aforementioned Affidavit. Based on that conversation, I know the following about SUBJECT PREMISES #1 and SCHEMER#13:

a. As discussed in the aforementioned Affidavit in support of the search warrant for SUBJECT PREMISES #1, this investigation has identified SCHEMER#13 as one of the runners in the scheme. SA Yepez and other federal law enforcement officers have observed SCHEMER#13 transport and/or accompany other schemers to and from SUBJECT PREMISES #1 to banks and private mail box locations to open accounts and mail boxes that are used in the scheme.

b. As discussed in the aforementioned Affidavit, SA Yepez and other agents have seen SCHEMER#13 on the balcony of SUBJECT PREMISES #1 on more than 20 different occasions since August 3, 2015. SA Yepez has also seen SCHEMER#13 engage in conversations with other schemers on the balcony of SUBJECT PREMISES#1, including: SCHEMER#1, the suspected ring leader, SCHEMER#8, SCHEMER#9, SCHEMER#12, SCHEMER#14, SCHEMER#15, SCHEMER#16, and UF1 (Unknown Female). In fact, SA Yepez saw

SCHEMER#13 engage in conversations with SCHEMER#1, SCHEMER#8, SCHEMER#9, and SCHEMER#12 on the balcony of SUBJECT PREMISES#1, as recent as Tuesday, April 19, 2016.

c. As discussed in the aforementioned Affidavit, SUBJECT PREMISES #1 is hub used by the schemers to operate their money laundering scheme. SA Yepez has seen SCHEMER#13 open SUBJECT PREMISES #1 using what appears to be an apartment key on different occasions. SA Yepez has also seen SCHEMER#13 close the blinds of SUBJECT PREMISES #1, turn off the apartment lights there, and exit SUBJECT PREMISES #1 with other schemers, including with SCHEMER#1. Based on SA Yepez's surveillance of SUBJECT PREMISES #1, SA Yepez believes SCHEMER#13 has unlimited access to SUBJECT PREMISES #1 and is responsible for opening, closing, and securing it, which would render him a trusted member of this scheme.

d. SA Yepez also believes that SCHEMER#13 currently resides in the Avalon Apartments complex, albeit in a different apartment there, specifically in building 10945. (SUBJECT PREMISES #1 is located in building 10987 of the Avalon Apartments complex.) HSI Special Agent Michael Ou and SA Yepez have seen SCHEMER#13, SCHEMER#8, and a suspected schemer unknown to the investigation use a fob key to enter building 10945 at the Avalon Apartments complex. For example, on December 7, 2015, SA Yepez observed SCHEMER#8 and SCHEMER#13 access the front door of building 10945. Based on SA Yepez's conversations

with the Avalon Apartments complex leasing manager, and his personal experience, SA Yepez knows that Building 10945 can only be accessed with a fob key, which is assigned to every tenant. As discussed in the aforementioned affidavit, SA Ou and SA Yepez followed SCHEMER#8 and SCHEMER#13 from SUBJECT PREMISES#1 to the Citibank located at 1900 W. Sunset Blvd., Los Angeles, California, where SCHEMER#8 entered the bank and identified himself to the bank manager as "Hrant Abovyan." At that time, SCHEMER#8 provided a fraudulent passport in the name of "Hrant Abovyan" and closed out the account and as a result received a cashier's check. During this time SCHEMER#13 waited outside the bank. SA Ou and SA Yepez observed SCHEMER#8 exit the bank with a document and enter the passenger side of SCHEMER#8's vehicle. SCHEMER#13 was the driver. SA Ou and SA Yepez attempted to follow SCHEMER#13; however, surveillance ended once SCHEMER#13 was observed conducting counter surveillance techniques. SA Yepez later learned that SCHEMER#8 had deposited the cashier's check into another Tier-2 bank account at East West Bank account located near the Citibank branch. SA Ou also told SA Yepez that he had observed SCHEMER#13 enter building 10945 of the Avalon Apartment complex through a side door located east of the main entrance of building 10945.

e. In addition, on April 15, 2016, SA Ou conducted a surveillance operation of the Avalon Apartments complex and of SUBJECT PREMISES #1. During the surveillance operation, SA Ou

told SA Yepez that he had observed SCHEMER#1 exit the Avalon Apartments complex through the eastside gate with an unknown male adult who had been seen in SUBJECT PREMISES #1 earlier in the day with SCHEMER#1. SA Ou told SA Yepez that SCHEMER#1 was holding SUBJECT BAG #1 while he was walking with the unknown individual. SCHEMER#1 and the unknown male stopped approximately 10 feet from SA Ou's vehicle and began talking to each other for approximately 10 minutes. SA Ou then observed the unknown male enter the main entrance of building 10945 with a fob key, while SCHEMER#1 entered SUBJECT VEHICLE #1 with SUBJECT BAG #1.

f. SA Yepez provided the Leasing Manager of the Avalon Apartments complex the true name of SCHEMER#13 to run in their databases in order to determine whether SCHEMER#13's true name was listed as an active resident. SA Yepez was told by the Avalon Apartments complex personnel that they did not have any records that show anyone in the true name of SCHEMER#13 lives at the Avalon Apartments complex.

g. SA Yepez also interviewed four Avalon Apartments complex employees, three of which themselves rent apartments in building 10945 there. All four employees told SA Yepez that they have seen SCHEMER#13 smoking outside building 10945, inside building 10945, in the underground parking structure of building 10945 with other Armenian males, and at the Starbuck's located on the corner of Vineland Ave. and Ventura Blvd., which is approximately 0.2 miles from SUBJECT PREMISES #1.

h. Based on the above, SA Yepez and I believe that SCHEMER#13 residence in an apartment in building 10945 at the Avalon Apartments complex or an apartment that can be accessed from building 10945 there.

i. Based on the above, and our training and experience, SA Yepez and I believe that there will be evidence in this scheme stored in SCHEMER#13's residence at the Avalon Apartments complex, because, among other things, SCHEMER#13 has been observed with other known schemers on a daily business at SUBJECT PREMISES#1; SCHEMER#13 has been accessing SUBJECT PREMISES #1 with a key, which shows he is a trusted schemer; SCHEMER#13 has been observed transporting schemers to and from SUBJECT PREMISES#1 to conduct fraud related to the scheme, such as to banks; SCHEMER#13 has been observed driving vehicles not registered to him and conducting counter surveillance; and the Avalon Apartments complex do not have records reflecting that SCHEMER#13 is renting an apartment there, even though it appears that SCHEMER#13 does in fact reside at an apartment in the Avalon Apartments complex.

IV. Training and Experience on Digital Devices

13. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital

data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded

onto a hard drive, deleted, or viewed via the Internet.

Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive

requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and

the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

V. CONCLUSION

14. For all the reasons described above, there is probable cause to believe that evidence of violations of Title 18, United States Code, Sections 286, 287, 371, 1001, 1028(a)(7), 1343, 1344, and 1956, which criminalize, respectively, conspiracy to defraud the United States with respect to claims, false claims, conspiracy to defraud the United States, making or using false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry, identity theft, wire fraud, bank fraud, and money laundering, as described above and in Attachment B of this affidavit, will be found in a search of SUBJECT LAPTOP #1, SUBJECT LAPTOP #2, SUBJECT LAPTOP #3, SUBJECT LAPTOP #4, SUBJECT LAPTOP #5, SUBJECT LAPTOP #6, SUBJECT LAPTOP #7, SUBJECT LAPTOP #8, SUBJECT LAPTOP #9, SUBJECT LAPTOP #10, SUBJECT LAPTOP #11, and SUBJECT IPAD #1, as further described above and in Attachments A-1 to A-12 to this affidavit.

57

Leia Bellis, Special Agent
Internal Revenue Service - Criminal
Investigation

Subscribed to and sworn before me
this 21 day of April 2016

151

~~HONORABLE ALKA SAGAR~~
UNITED STATES MAGISTRATE JUDGE

KAREN E. SCOTT

25

[Instrumentality Protocol]

ATTACHMENT A-1

PREMISES TO BE SEARCHED

A black-colored laptop, Dell model Latitude, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #32 (SUBJECT LAPTOP #1).

ATTACHMENT A-2

PREMISES TO BE SEARCHED

A silver-colored laptop, Lenovo model Ideapad 100S, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #29 (SUBJECT LAPTOP #2).

ATTACHMENT A-3

PREMISES TO BE SEARCHED

A black-colored laptop, Toshiba model Satellite, located on right side of the desk in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #30 (SUBJECT LAPTOP #3).

ATTACHMENT A-4

PREMISES TO BE SEARCHED

A blue-colored laptop, HP model Stream, located on the floor in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #59 (SUBJECT LAPTOP #4).

ATTACHMENT A-5

PREMISES TO BE SEARCHED

A silver-colored laptop, HP model Notebook, located on the floor in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #54 (SUBJECT LAPTOP #5).

ATTACHMENT A-6

PREMISES TO BE SEARCHED

A black-colored laptop, Dell, located on the floor in the sole bedroom of SUBJECT PREMISES #1, on top of a printer, marked by agents as Digital Device #55 (SUBJECT LAPTOP #6).

ATTACHMENT A-7

PREMISES TO BE SEARCHED

A black-colored laptop, Toshiba model Satellite, located on a shelf in the closet in the sole bedroom of SUBJECT PREMISES #1, marked by agents as Digital Device #60 (SUBJECT LAPTOP #7).

ATTACHMENT A-8

PREMISES TO BE SEARCHED

A black-colored laptop, Toshiba model Satellite, located with SUBJECT LAPTOP #7 on a shelf in the closet in the sole bedroom of subject of SUBJECT PREMISES #1, marked by agents as Digital Device #61 (SUBJECT LAPTOP #8).

ATTACHMENT A-9

PREMISES TO BE SEARCHED

A black-colored laptop, Lenovo model Ideapad 100, located on a folding table near the front door of SUBJECT PREMISES #1, marked by agents as Digital Device #1 (SUBJECT LAPTOP #9).

ATTACHMENT A-10

PREMISES TO BE SEARCHED

A black-colored laptop, Dell, located on a folding table near the front door of SUBJECT PREMISES #1 with SUBJECT LAPTOP #9, marked by agents as Digital Device #2 (SUBJECT LAPTOP #10).

ATTACHMENT A-11

PREMISES TO BE SEARCHED

A black-colored laptop, HP model Notebook, located on a bookshelf in the main room of SUBJECT PREMISES #1, inside a box, marked by agents as Digital Device #3 (SUBJECT LAPTOP #11).

ATTACHMENT A-12

PREMISES TO BE SEARCHED

A black Ipad, with a silver back, located on the desk near SUBJECT LAPTOP #1 under some papers, marked by agents as Digital Device #53 (SUBJECT IPAD #1).

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 286, 287, 371, 1001, 1028(a)(7), 1343, 1344, and 1956, which criminalize, respectively, conspiracy to defraud the United States with respect to claims, false claims, conspiracy to defraud the United States, making or using false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry, identity theft, wire fraud, bank fraud, and money laundering, namely:

a. For the time period 2011 to present, for both domestic and foreign financial institutions: account opening documents, applications, signature cards, bank records, financial account records, time deposit records, bank statements, brokerage statements, certificates of deposits, wire transfer records, currency records, mutual fund records, cancelled checks, check books, withdrawal slips, deposit slips, cashier checks, negotiable items, travel checks, bearer instruments, western union information, commercial money transmitter records, money orders, money order receipts, loan documents, credit card records, credit cards, debit cards, bank cards, Pre-paid debit cards, records pertaining to the loading of pre-paid debit cards, bank correspondence, non-U.S. Citizen documents generally used to open bank accounts or to facilitate

[Instrumentality Protocol]

business transactions, such as Forms W-8, Forms W-8Ben, Forms WW-8Ben-E;

b. Tax returns, including originals or copies of completed federal income tax returns for the tax years 2010, 2011, 2012, 2013, 2014, and 2015, (Forms 1040, 1040A, 1040EZ, 1040 PC, 1040X, and electronically filed versions of the same) including all schedules, attachments, and forms; worksheets and/or supporting documentation used in the preparation of tax returns; and other documents used in the creation and/or preparation of the above mentioned tax returns, and tax-related documents, including:

i. IRS publications, regulations, and/or copies of IRS forms and documents; extracts from the Internal Revenue Code; and any correspondence relating to IRS forms, Internal Revenue Statutes or regulations and tax schedules.

ii. Documents or materials related to training in tax law and/or the preparation of tax returns, including training manuals, computer software, sample returns, templates, and correspondence in electronic, video, and paper formats.

iii. Records relating to federal income tax refunds, specifically, U.S. Treasury checks, wire transfers, cashier's checks, check stubs, check receipts, check inquiries, invoices, and direct deposit information.

c. Passport-related documents, from the United States of America, the Republic of Armenia, the Republic of Uzbekistan, Georgia, Kazakhstan, Russian, and any other country, including:

[Instrumentality Protocol]

i. Passport Books, Passport Cards, travel records, visa stamps, visa stickers, arrival stamps and departure stamps.

ii. Altered or false passport-related documents, including Passport Books, Passport Cards, photo copies of passports, blank passports, or any other document that appears to be issued by a government and used to verify identity or citizenship.

iii. Driver's licenses and related documents including those issued by any state of the United States or any foreign driver's license including an international driver's license, as well as altered or false such documents;

d. Records, lease agreements, registration, and utility bills for services, including electric, gas, trash services, water, cable, satellite television, telephone services, cellular phone services, and internet services, and any altered or fabricated such documents;

e. Shopping membership cards, including those issued by Costco, Vons, CVS, or any similar business entity, and any records regarding same, including membership applications, billing records, and communications;

f. Post office box rental records and commercial mail box rental records, including records of payments, applications, receipts, e-mail messages, and other communications;

g. Accounts receivable ledgers, commission ledgers, accounts payable ledgers, names and telephone numbers of co-

[Instrumentality Protocol]

conspirators, notes, other ledgers, journals, telephone bills, bank records, loan documents, day planner records, travel records, money ledgers, customer lists, currency supplier lists, correspondence, notations, logs, receipts, financial records, and other documents noting the source, destination, quantity, value, and/or purpose of currency obtained, transferred, deposited, wired, distributed, structured or concealed. Telephone and address books and listings, letters, cables, telegrams, telephone bills, personal notes and other items reflecting names, addresses, telephone numbers, communications.

h. Cash in excess of \$1,000;

i. Gold in any form including gold coins, gold bars, gold jewelry, and certificates of gold,

j. Financial instruments purchased with large amounts of currency including traveler's checks, wire transfers, bonds, stock certificates, cashier's checks and certificates of deposit;

k. Receipts and other documents relating to the purchase of assets with currency in amounts over \$10,000;

l. Records, receipts, invoices, shipping instructions, shipping receipts, packaging material, masking agents, shipping containers and labels, reflecting the use of either the U.S. mails or commercial delivery services (such as FedEx, and UPS) to facilitate the shipment of gold, currency, checks, or bearer instruments;

m. Safe deposit box keys and records of safe deposit box rentals, locations and access;

[Instrumentality Protocol]

n. Records and documents relating to Gold Depot, Newport aka Gold Exchange or Precious metals;

o. For the time period 2011 to present, records, deeds, lease agreements, registration, utility bills, and any other documentation showing ownership or control of: (1) 10987 Bluffside Drive, Apartment #4209, Studio City, California 91604; (2) Non Stop Wireless, which is a wireless service provider business located at 12901 Sherman Way, Suite A, North Hollywood, California 91605; or (3) 22745 Macfarlane Drive, Woodland Hills, California 91364;

p. Any documents that appear to be written in the Armenian, Russian, or Georgian languages that the searching agents believe may be within the scope of items to be seized. Because it is possible that none of the searching agents will have the ability to read records written in foreign languages listed above, these documents will be reviewed by an interpreter each respective language as soon as practicable, and if these documents are outside of the scope of the items to be sized, they will be returned within 60 days.

q. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

r. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were

[Instrumentality Protocol]

created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser

[Instrumentality Protocol]

history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant

[Instrumentality Protocol]

will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

[Instrumentality Protocol]

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

[Instrumentality Protocol]

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if: the device is determined to be an instrumentality of an offense under investigation or] the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device. If the search determines that a digital device contains data falling within the list of items to be seized, the government may also retain the device itself, without further order of the Court.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

[Instrumentality Protocol]

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

[Instrumentality Protocol]

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

[Instrumentality Protocol]

Attachment

C

UNITED STATES DISTRICT COURT

for the
Central District of CaliforniaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)10987 Bluffside Drive, Unit 4209
Studio City, California 91604

Case No.

SA 16-174M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-1

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, United States Code, Sections 286, 287, 371,
1001, 1028(a)(7), 1343, 1344, and 1956.

Offense Description

See attached Affidavit

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.15/
Applicant's signature

Adrian Yopez, Special Agent (IRS-CI)

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/19/16

15/
Judge's signature

KAREN E. SCOTT

Karen E. Scott, U.S. Magistrate Judge

Printed name and title

City and state: Santa Ana, California

AUSA: C. Pell

CEP

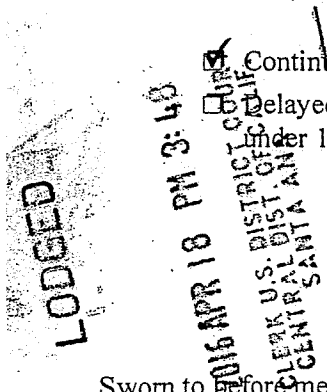
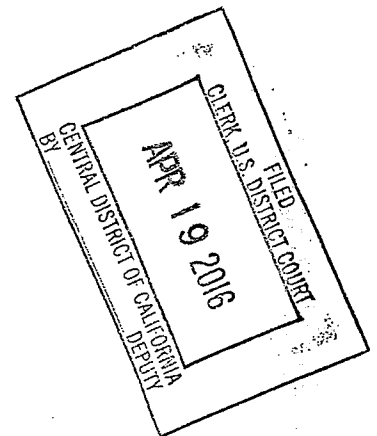


TABLE OF CONTENTS

<u>DESCRIPTION</u>	<u>PAGE</u>
I. INTRODUCTION	1
II. PURPOSE OF AFFIDAVIT	2
III. STATEMENT OF PROBABLE CAUSE	4
A. Summary of Investigation	4
B. Money Laundering Using Three Tiers of Bank Accounts	5
C. Stolen Identity Refund Fraud ("SIRF") schemes	7
1. ITC#127	7
2. ITC#298	8
3. Common links between ITC#127 and ITC#298	8
D. Training and experience regarding records related to a SIRF scheme.	9
E. Tier-1, Tier-2, and Tier-3 Bank Accounts	11
1. Tier-1 bank accounts	11
2. Tier-2 bank accounts	13
3. Tier-3 bank accounts	14
F. Money Laundering Schemes Related to This Scheme	23
1. FBI health care money laundering sting investigation involving Gagik Airapetian ("SCHEMER#1")	23
2. IRS-CI and FBI Seattle tax fraud investigation	28
G. The Use of Private Mailboxes to Facilitate Money Laundering	29
H. Identified Schemers in This Investigation	31
1. SCHEMER#1: Gagik Airapetian	31
2. SCHEMER#2: Karen Pogolian	33

3.	SCHEMER#3: Armen Mkrtchyan	37
4.	SCHEMER#4: Sargis Tabadzhyan, AKA "Sergio Tabadzhyan"	41
5.	SCHEMER#5: Hripsime Avagyan	49
6.	SCHEMER#6: Jane Doe	54
7.	SCHEMER#7: Artash Stepanyan	58
8.	SCHEMER#8: Eduard Astvatsatryan	64
9.	SCHEMER#9: John Doe	70
10.	SCHEMER#10: Konstantin Galstyan	73
11.	SCHEMER#11: Mkhitar Mkrtchyan	77
12.	Other conspirators/schemers	82
a.	SCHEMER#12: Marat Nazaryan	82
b.	SCHEMER#13: Arman Abrahamyan	84
c.	SCHEMER#14: Harutyun Sukiasyan	86
d.	SCHEMER#15: Albert Andriasov	87
e.	SCHEMER#16: Tigran Galstyan	90
f.	SCHEMER#17: Haroutioun Demirdjian	92
I.	During 2015, Chic Accessories, a Business in Hollywood, California, Was The Meeting and Storage Location From Which Various Schemers Originated Before Depositing Tier-1 Checks into Tier-2 Bank Accounts As Part of This Scheme. .	94
J.	There is Probable Cause to Believe That Evidence of This Scheme Will be Found at SUBJECT PREMISES #1, Which Is An Apartment Used as a Hub of Operations and Meeting Place for the Schemers.	99
1.	Introduction and Summary	99
2.	Tier-2 bank account holders use SUBJECT PREMISES #1 as part of this scheme.	107

K.	There Is Probable Cause To Believe That Evidence of This Scheme Will Be Found at Non Stop Wireless aka "NS Wireless" (SUBJECT PREMISES #2)	147
1.	SUBJECT PREMISES #2 was used by SCHEMER#1 in 2012 to launder proceeds from health care fraud.	148
2.	The owners/operators of the business at SUBJECT PREMISES #2 are also involved in this scheme.	149
3.	SUBJECT PREMISES #2 is used in this scheme.	153
L.	There Is Probable Cause To Believe That Evidence of This Scheme Will Be Found At SUBJECT PREMISES #3.	156
M.	There is Probable Cause to Believe That Evidence of This Scheme Will Be Found in SUBJECT VEHICLE #1, Which Is SCHEMER#1's Vehicle.	168
N.	There Is Probable Cause To Believe That Evidence of This Scheme Will Be Found In SUBJECT BAG #1, Which Is The Satchel That SCHEMER#1 Routinely Carries With Him in This Scheme.	171
O.	The use of computers and digital devices in the scheme ..	174
IV.	CONCLUSION	178

A F F I D A V I T

I, Adrian Yepez, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the Internal Revenue Service - Criminal Investigation ("IRS-CI"), assigned to the Los Angeles Field Office, and have served in this capacity since April 2010. As part of my training as an SA, I attended the Federal Law Enforcement Training Center in Glynco, Georgia, where I received training in criminal and financial investigative techniques with an emphasis in accounting and criminal tax law. My training included courses in law enforcement techniques, federal criminal statutes, criminal investigations, execution of search warrants, financial investigative techniques, and legal principles and statutes representing criminal violations of Titles 18, 26, and 31 of the United States Code. My formal education includes a Bachelor of Arts degree in Law and Society with an emphasis in Criminal Justice from the University of California, Santa Barbara. I have personally conducted and assisted in investigations of criminal violations of the Internal Revenue laws, the Bank Secrecy Act, the Money Laundering Control Act, identity theft, bank fraud, credit card fraud, wire fraud, and healthcare fraud. These investigations have involved the use of electronic and physical surveillance; the use of informants and cooperating witnesses; undercover operations; and the preparation and execution of search and arrest warrants. In addition to the

training described above, I have attended training seminars and meetings related to the investigation of financial crimes, including identity theft investigations. From October 2013 to October 2015, I was the Identity Theft Coordinator for the IRS-CI Los Angeles Field Office. In that capacity, my duties included investigating stolen identity refund fraud schemes, developing identity theft leads from local, state, and federal law enforcement agencies, participating in state and federal Identity Theft Task Forces, and acting as the Identity Theft liaison for the IRS.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of an application for warrants to search for evidence of violations of Title 18, United States Code, Sections 286, 287, 371, 1001, 1028(a)(7), 1343, 1344, and 1956, which criminalize, respectively, conspiracy to defraud the United States with respect to claims, false claims, conspiracy to defraud the United States, making or using false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry, identity theft, wire fraud, bank fraud, and money laundering.

3. The locations, car, and bag to be searched are:

a. 10987 Bluffside Drive, Apartment #4209, Studio City, California 91604, which is a one bedroom apartment located on the second floor of building 10987 of the Avalon Apartments ("SUBJECT PREMISES #1"), as more fully described in Attachment A-1;

b. Non Stop Wireless, which is a wireless service provider business located at 12901 Sherman Way, Suite A, North Hollywood, California 91605 ("SUBJECT PREMISES #2"), as is more fully described in Attachment A-2;

c. 22745 Macfarlane Drive, Woodland Hills, California 91364, which is a two story, four bedroom, three bathroom, three thousand square foot single family residence ("SUBJECT PREMISES #3"), as more fully described in Attachment A-3;

d. A Grey 2008 Acura MDX with California license plate number 7HUW657 and Vehicle Identification Number 2HNYD28398H519552, registered to Gagik Airapetian at 22745 Macfarlane Drive, Woodland Hills, California 91364 ("SUBJECT VEHICLE #1"), as more fully described in Attachment A-4; and

e. A black or dark colored bag possessed by Gagik Airapetian, described as a satchel, computer bag, or messenger bag, with a strap that is attached on each end that is carried over the shoulder, ("SUBJECT BAG #1"), as more fully described in Attachment A-5.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated

otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. STATEMENT OF PROBABLE CAUSE

A. Summary of Investigation

5. IRS-CI and the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), have been investigating a large fraud ring that has been laundering tens of millions of dollars in tax refunds that were fraudulently obtained from false federal tax returns that had been filed using stolen identities.

6. Tax fraud: In this scheme, for tax years 2012, 2013, and 2014, the IRS has identified approximately 7,000 false tax returns that together fraudulently claimed approximately \$38,000,000 in refunds, of which approximately \$14,000,000 was deposited into and laundered through bank accounts used in this scheme. Millions of dollars more were deposited and laundered from 2010 to 2016.

7. Identity theft: The false tax returns were filed using stolen identity information from thousands of victims. The schemers discussed below also used approximately 200 fraudulent identities with corresponding fraudulent identification, including passports from the Republic of Armenia, to open hundreds of mailbox addresses and bank accounts in those other individuals' identities.

8. Money laundering: The schemers then used those hundreds of mailbox addresses and bank accounts to launder the millions of dollars in ill-gotten tax refunds by transferring the funds among three levels (or "tiers") of bank accounts, in an apparent effort to render the funds ultimately untraceable. Some of the funds were wire transferred internationally, including to bank accounts located in the Republic of Armenia.

B. Money Laundering Using Three Tiers of Bank Accounts

9. Generally, money laundering is the process of taking the proceeds of criminal activity and "laundering" (or "washing") those proceeds, in order to make them appear as if originating from legal activity. The money laundering process can be broken down into three distinct stages: placement, layering, and integration.

10. The money laundering process in this investigation occurred in the following manner, using three tiers of bank accounts. A fraudulent tax return seeking a refund is initially filed using stolen identity information.

11. First, tax refunds from the fraudulent tax returns are direct deposited by the IRS into bank accounts ("Tier-1 bank accounts") that were opened in the names of individuals and businesses that differ from those in which the fraudulent tax returns were filed. This is commonly known as the "placement process" of money laundering.

12. Second, in order to extract the funds from the Tier-1 bank accounts, checks from those Tier-1 bank accounts are then

written to individuals and businesses and deposited into their bank accounts ("Tier-2 bank accounts"), which are themselves also opened generally using fictitious/stolen identities. This is commonly known as the "layering process" of money laundering.

a. In order to facilitate the fraud and opening of Tier-1 and Tier-2 bank accounts, which are basically money laundering accounts, the fraudsters open Private Mailboxes ("PMB") at commercial mail receiving agencies ("CMRA"), such as a UPS Store.

b. Generally, such PMBs were opened using suspected fraudulent passports along with other documents that included Costco membership cards, or utility bills that appear to be altered. The passports used to open the PMBs or bank accounts purport to be issued from the Republic of Armenia, the country of Georgia, and the Czech Republic, as well as other European countries.

13. Third, checks from Tier-2 bank accounts are then written to other Tier-2 bank accounts for additional layering, or to actual businesses and individuals operating as gold and precious metal wholesalers ("Tier-3 bank accounts"). This is commonly known as the "integration process" of money laundering.

14. After the funds are received into the Tier-3 bank accounts, e.g., the gold and precious metal wholesalers, the laundering is complete, and the disposition of the funds is unknown.

C. Stolen Identity Refund Fraud ("SIRF") schemes

15. Stolen identity refund fraud involves a fraudulent claim or attempted claim for a tax refund wherein the fraudulent claim for refund (i.e., tax return) is filed in the name of a person whose personal identification information appears to have been stolen or unlawfully used to make the claim, and the claim is intended to benefit someone other than the person to whom the personal identification information belongs.

16. As described below, the identities used to file the false tax returns in this scheme were obtained in at least two different ways.

1. ITC#127

17. Approximately half of the identities used to file the false tax returns in 2014 were stolen from data breaches of five professional tax return preparers located in Los Angeles County. IRS SAs, including me, interviewed the return preparers and learned that their clients' profiles and tax data had been stolen and were used to file false tax returns in 2014.

18. During 2014, approximately 800 such fraudulent tax returns were filed electronically from one IP address, which together claimed approximately \$7,000,000 in tax refunds. The IRS issued approximately \$2 million of the \$7 million in refunds that had been claimed.

19. All of the tax refunds were direct deposited into over 100 different Tier-1 bank accounts. The IRS identified this scheme as "ITC #127." ("ITC" stands for the IRS's "Identity

Theft Clearinghouse," which is responsible for researching and identifying identity theft refund fraud schemes.)

2. ITC#298

20. The other half of the identities used in this scheme were obtained in an unknown manner but were identified through common IP addresses and bank accounts. The identity theft victims appear to be located all across the United States, including in 49 states. IRS Identity Theft Clearinghouse identified this scheme as "ITC#298."

21. During 2014, approximately 849 false federal tax returns were filed in ITC#298 claiming approximately \$7,000,000 in tax refunds. The IRS issued over \$4,000,000 of those refunds.

22. Unlike scheme ITC#127, several different IP addresses were used to transmit the false tax returns in scheme ITC#298. These IP addresses were traced back to Henderson, Nevada; Philadelphia, Pennsylvania; and Tampa Bay, Florida.

23. All of the tax refunds in ITC#298 were electronically deposited into approximately 100 different Tier-1 bank accounts used in this scheme.

3. Common links between ITC#127 and ITC#298

24. The Tier-1 bank accounts (i.e., the bank accounts into which the fraudulently obtained tax refunds were deposited) used in ITC#127 and ITC#298 in 2014 are distinct. However, the Tier-2 and Tier-3 bank accounts used in the two schemes are common to laundering the money from both schemes.

25. IRS Investigative Analyst ("IA") Dan Gilmore identified approximately 1,600 false tax returns that were filed with the IRS in 2015 that he believes are related to ITC#298. Those filed tax returns claimed refunds of approximately \$10,000,000. Approximately \$5,000,000 of the \$10,000,000 in refunds that were claimed was electronically deposited into Tier-1 bank accounts.

26. Additional research identified more fraudulent tax returns filed in 2012 and 2013 that were laundered using known Tier-1 and Tier-2 bank accounts during 2014.

D. Training and experience regarding records related to a SIRF scheme.

27. I have conducted and participated in, and discussed with other agents who have conducted, investigations into SIRF schemes. Moreover, I have conducted and participated in, and discussed with other agents who have conducted, investigations involving false tax returns.

28. Based on my training and experience, including training and experience when I was the Identity Theft Coordinator for IRS-CI, I know that a person engaged in a stolen identity tax refund fraud will almost always maintain some or all of the following types of the following records: list or spreadsheet containing personal identifying information; social security numbers, employee identification numbers; addresses, bank records, to include routing and account numbers, bank statements, cancelled checks, deposit slips, wire transfer

receipts, and bank correspondences; email addresses, and phone records; cash receipts; summary sheets or schedules showing total refunds received; communication records between the schemers to include notes detailing instructions and comments; profile lists; tax returns; tax forms such as Forms W-2s, copies of post office applications, foreign passports and visas, and computer and computer storage devices containing any or all of the above information. I also know, based on my training and experience, with respect to small business owners, that the above referenced records may be located at the business location or storage unit, as well as often taken to the residence of the leaders or managers of the identity theft or tax fraud schemes.

29. Based on my training and experience, including training and experience when I was the Identity Theft Coordinator for IRS-CI, I know that in addition to keeping records of the scheme at the business or residence locations used in the scheme, the schemers often carry on their person, often located in containers such as handbags, documents used in the scheme, such as copies of the fraudulent tax returns, the fraudulent identifications, and other documents described in the preceding paragraph.

E. Tier-1, Tier-2, and Tier-3 Bank Accounts

1. Tier-1 bank accounts

30. As described above, "Tier-1 bank accounts" are bank accounts used to directly receive the fraudulently obtained tax refunds from the IRS.

31. I have reviewed hundreds of Tier-1 bank account records received from various financial institutions. These records include opening account documents, bank statements, deposited items, and cancelled checks drawn on the bank accounts. In reviewing the Tier-1 bank account records, I found that the accounts generally share the following characteristics:

a. The addresses provided by the account holders generally turned out not to be physical addresses or residences, but rather, addresses for private mailboxes. Others are foreign addresses, and some are residential and business addresses in the United States.

b. Some of the bank accounts are in the name of individuals who used their true identities.

c. Tier-1 bank accounts were often opened using passports purportedly issued from the Republic of Armenia, the country of Georgia, Russia, the Czech Republic, and other European countries.

d. The tax refunds deposited into the Tier-1 bank accounts were not issued in the name of the bank account holder.

e. Multiple Tier-1 bank accounts were opened by the same person using the same identity and private mailbox address.

Sometimes that same person would also open additional bank accounts posing in different identities.

f. Most of the bank accounts were opened six months to one year prior to the deposits of the tax refunds.

g. The bank accounts remained inactive until the accounts began to receive the tax refunds.

h. The activity in the bank accounts consists of an opening cash deposit, deposits of tax refunds in other people's names, and withdrawals, usually in the form of checks written to Tier-2 bank accounts.

i. A Tier-1 bank account may be used in multiple tax years as a Tier-1 bank account.

32. Some of the tax refunds that were deposited into the Tier-1 bank accounts were frozen by the financial institutions based on the suspicion of identity theft and tax fraud, and the proceeds were returned to the IRS. In other cases, the financial institutions froze the bank accounts but did not return the funds to the IRS.

33. International wire transfers from Tier-1 bank accounts: I reviewed bank records for Tier-1 bank accounts used in the scheme and discovered multiple outgoing wire transfers to banks located in the Republic of Armenia. Specifically, at least 19 different individuals were listed as beneficiaries of the outgoing wires. All of the names of beneficiaries appear to have Armenian surnames.

2. Tier-2 bank accounts

34. As described above, "Tier-2 bank accounts" are accounts used for layering the illicit tax fraud proceeds.

35. I have reviewed hundreds of Tier-2 bank account records received from various financial institutions. These records include opening account documents, bank statements, deposited items, and cancelled checks drawn on the bank account. In reviewing the Tier-2 bank account records, I found that the bank accounts share the following characteristics:

a. The account holders provided addresses that were either private mailboxes or were addresses that were provided to private mailbox stores, also known as Commercial Mail Receiving Agencies ("CMRAs") when they opened the private mailboxes. The addresses provided are not where the individuals actually reside. In some instances, the addresses have been confirmed to be fictitious or nonexistent.

b. Tier-2 bank account holders generally open the bank accounts using fictitious/stolen identities.

c. Tier-2 bank accounts were often opened using passports from the Republic of Armenia, the country of Georgia, the Czech Republic, and other European countries.

d. The activity in the Tier-2 bank accounts generally consists of deposits of checks drawn on Tier-1 and other Tier-2 bank accounts followed by checks made payable to other Tier-2 and Tier-3 bank accounts. In some instances, cash withdrawals were made in the branch or using ATM machines by

various runners in the scheme. Generally, the Tier-2 bank accounts do not have any other significant activity. From my review, it appears the sole purpose of those accounts is to layer funds.

e. Multiple Tier-2 bank accounts were opened by the same person using the same identity. That same person using a different identity often opened other accounts.

36. Occasionally, a Tier-1 bank account used during one year subsequently becomes a Tier-2 bank account in a later year.

37. A Tier-2 bank account may be used in multiple years as a Tier-2 bank account.

3. Tier-3 bank accounts

38. Tier-3 bank accounts are described in this affidavit as business bank accounts opened by real individuals who claim to be owners of jewelry companies. The jewelry companies generally have addresses in the Los Angeles "Jewelry District" area, which is located in downtown Los Angeles, California.

39. IRS SA Leonard and I analyzed the checks drawn on several of the Tier-2 bank accounts and learned that the majority of the checks from those bank accounts were made payable to the following business entities: Unika Jewelry, L.A. Hoops, H.D. Jewelry, M&M Jewelry, and Zig Zag Jewelry. These companies held business bank accounts at various banks including Citibank, Comerica Bank, East West Bank, Wells Fargo, Hanmi Bank, Pacific Western Bank, and HSBC Bank.

40. Zig Zag Jewelry: I have reviewed records for Citibank account number 203591979 in the name of Zig Zag Jewelry, which I obtained by federal Grand Jury subpoena. The documents provided by Citibank show that a business bank account in the name of Zig Zag Jewelry was opened on or about April 13, 2010. Mkhitar Mkrtchyan (discussed below as SCHEMER#11) is listed as the authorized signer on the bank account and as the President of Zig Zag Jewelry.

a. IRS SA Leonard conducted a deposit and check analysis of account number 203591979 for the time period of February 2014 to May 2014. I have reviewed SA Leonard's analysis and confirmed that during those months, approximately \$1.17 million in checks drawn on Tier-2 bank accounts were deposited into SCHEMER#11's Zig Zag bank account. I also learned that from January 2014 to May 2014, SCHEMER#11 made checks payable from the Zig Zag bank account to Gold Depot and Newport Precious Metals for a total of approximately \$975,000.

b. Kenneth Koyama, HSI Forensic Accountant working for Homeland Security, conducted an analysis of account number 203591979 for 2012 and 2013. I have reviewed his analysis and, for those two years, found similar activity as the activity during 2014 described above. This includes checks deposited that were drawn from known and suspected Tier-2 bank accounts. According to his analysis of this bank account, checks totaling approximately \$333,000 were written to B.A.K. Precious Metals Inc. and Newport Precious Metals Inc. in 2013, and in 2012,

approximately \$600,000 to B.A.K. Precious Metals Inc. and Newport Precious Metals Inc.

c. I reviewed records for Umpqua Bank account number 9804809391. The signature card shows that the account was opened on March 27, 2015, in the name of Zig Zag Jewelry. SCHEMER#11 is listed as the sole account holder and owner of Zig Zag Jewelry. My review of Umpqua Bank records for bank account number 9804809391 showed that during 2015, similar activity to that detailed above occurred. Such similarities include deposits consisting of incoming wire transfers from checks drawn on known Tier-2 bank accounts and a cashier's check, followed by checks made payable to Gold Depot and Newport Gold Exchange, for most of the amounts that had been deposited.

41. H.D. Jewelry: I have reviewed records of Hanmi Bank account number 500253169, which I obtained by federal Grand Jury subpoena. The signature card lists Haroutioun Demirdjian (discussed below as SCHEMER#17) as opening account number 500253169 on December 17, 2009. SCHEMER#17 is also listed as the sole owner and signer for the account. The bank account was opened under the name of "H.D. Jewelry, Inc." According to the signature card, SCHEMER#17 is listed as the President and Secretary of H.D. Jewelry.

a. IRS SA Leonard conducted a deposit and check analysis of account number 500253169 for the time period of February and March 2014. I have reviewed his analysis and found that for those two months, this account received deposits of

checks drawn from Tier-2 bank accounts, which totaled approximately \$173,000. The check analysis shows that during the same time period, H.D. Jewelry issued checks totaling \$86,775 to New Port Precious Metals. On April 2, 2014, SCHEMER#17's Hanmi Bank account was closed, and a cashier's check of \$63,782.90 was issued. I traced that cashier's check as being deposited to Comerica bank account number 1894328655. I subsequently obtained records for that bank account by federal Grand Jury subpoena. Upon reviewing those records, I observed that the signature card for Comerica bank account number 1894328655 lists SCHEMER#17 as the authorized signer on the account.

b. I have reviewed Comerica bank records for account number 1894328655 and found similar activity for 2012 through 2014. Specifically, deposits consisting of checks drawn from known and suspected Tier-2 bank accounts were made, followed by checks and wire transfers to Newport Precious Metals. I have reviewed an analysis of deposits and checks for account number 1894328655 for 2015 and found that over \$435,000 from checks drawn on Tier-2 bank accounts were deposited into the account. Subsequent to these deposits, the records show checks and wire transfers to Newport Gold Exchange for more than \$400,000.

42. Garro A. Minassian bank accounts: I reviewed records for East West Bank accounts 8031001921 and 2031004993, which were obtained pursuant to federal Grand Jury subpoena. The signature cards for both accounts list Garro A. Minassian as the

authorized signer and account holder for the accounts. Bank account 8031001921 was opened under the name Unika Jewelry Inc. DBA L.A. Hoops, on July 12, 2012. Minassian provided East West Bank with supporting documentation to show that he was the President of Unika Jewelry Inc. DBA L.A. Hoops. Bank account number 2031004993 was opened in the name of Garo A. Minassian.

a. Forensic Accountant Koyama conducted an analysis of account number 8031001921 for 2012, 2013, and 2014. His analysis reveals that between February 12, 2014, and June 13, 2014, a total of approximately \$900,000 in checks were deposited. Of that \$900,000, approximately \$875,000 came from checks drawn on Tier-2 bank accounts. The check analysis shows that for the same time period, checks totaling approximately \$715,000 made payable to Gold Depot were drawn on the account.

b. Forensic Accountant Koyama's analysis of the same account for 2012 and 2013 shows that the account was used in the same manner those years as it was during 2014. The deposits consist mostly of checks drawn on known and suspected Tier-2 bank accounts, just like in the time period discussed above. A large amount of those deposited funds was subsequently withdrawn from the bank account using checks payable to Gold Depot.

c. Forensic Accountant Koyama's analysis of bank account number 2031004993 for 2014 shows deposits that consist mostly of checks drawn from Tier-2 bank accounts. Most of the funds were then transferred to account number 8031001921.

d. I reviewed bank records from Pacific Western Bank for account numbers 13005885 and 1000051399, which I obtained by federal Grand Jury subpoena. The account opening documents show that Minassian opened the accounts on July 13, 2012, and April 5, 2011, respectively. The accounts were opened under the names Unika Jewelry Inc. DBA LA Hoops. The opening documents list Minassian as President of Unika Jewelry Inc. DBA LA Hoops, which is a jewelry wholesale business.

e. Analysis of bank accounts 13005885 and 1000051399 for 2012, 2013, and 2014 shows that those accounts were used in the same manner as the other Minassian bank accounts described above. The deposits consist mostly of checks drawn from known and suspected Tier-2 bank accounts, and large amounts of the funds so deposited were subsequently withdrawn from the account by checks payable to Gold Depot.

43. Moses Seraydarian bank accounts: According to law enforcement and IRS records and public information, including Secretary of State records, I know the following regarding Moses Seraydarian and his wife, Suzy Seraydarian:

a. Business "Chic Accessories" was incorporated in California in 2008 by Suzy Seraydarian and is located at 6519 Hollywood Blvd., Los Angeles, California 90028.

b. A search in the California Business Entity database shows that M&M Jewelry was incorporated in California on or about May 24, 2007. A status of "active" was shown as of

March 27, 2015, for the company. The agent for service was "Mouses Seraydarian."

c. A search in the California Business Entity data base shows that business Seray Jewelry was incorporated in California on or about February 13, 2013. A status of "active" was shown as of March 27, 2015, for the company. The agent for service was "Moses Seraydarian."

d. I have reviewed bank records for Pacific Western Bank account number 1000050334 in the name of M&M Jewelry. According to the signature card, "Movses Seraydarian" (sic) is the signer on the bank account and is listed as the president. The bank account was opened on June 13, 2007. The deposits in 2012 and 2013 to the bank account consist mostly of checks from known and suspected Tier-2 bank accounts. The majority of the funds were subsequently withdrawn from the bank account by checks made payable to Gold Depot.

e. I have reviewed bank records for Pacific Western Bank account number 1000051001 in the name of Chic Accessories. According to the signature card, Suzy Seraydarian is the signer on the bank account and is listed as the president. The bank account was opened on February 8, 2008. The deposits in 2012 and 2013 to the bank account consist mostly of checks drawn from known and suspected Tier-2 bank accounts. Subsequently, the majority of the funds were withdrawn from the bank account by checks for what appear to be business-related expenses such as rent, taxes, and utilities.

f.. I have reviewed bank records for Umpqua Bank account number 9921149788 in the name of Seray Jewelry Inc. According to the signature card, Moses Seraydarian is the signer on the bank account and is listed as the president. The bank account was opened on October 10, 2013. The deposits in 2015 to the bank account consist mostly of checks and cashier's checks drawn from known Tier-2 bank accounts. The majority of the funds were then withdrawn from the bank account by checks payable to Gold Depot.

g. I have reviewed bank records for Umpqua Bank account number 9885849985 in the name of M&M Jewelry Inc. According to the signature card, Moses Seraydarian is the signer on the bank account and is listed as the president. The bank account was opened on October 11, 2013. The deposits in 2014 and 2015 to the bank account consist mostly of checks drawn from known Tier-2 bank accounts. The majority of the funds were then withdrawn from the bank account by checks payable to Gold Depot.

44. Disposition of fraud proceeds after being deposited into Tier-3 bank accounts: I have reviewed a memorandum of interview written by another IRS-CI SA who spoke with the owner of Gold Depot, Kevork Kacharian, in 2011. In that interview, Kacharian stated that Gold Depot is a business involved in the buying and selling of precious metals such as gold, silver, platinum, as well as coins. Kacharian stated that BAK Precious Metals was previously a "big guy" in the industry, and that Newport Precious Metals was a business similar to Gold Depot.

a. California Secretary of State Business Entity database shows that Chad Hoang was the agent for service for Newport Precious Metals, Inc., located at 650 S. Hill St., #518A, Los Angeles, California 90014, which has since been dissolved.

b. California Secretary of State Business Entity database shows that Chad Hoang was the agent for service for Newport Gold Exchange, Inc., located at 650 S. Hill St., #518, Los Angeles, California 90014, which is active.

c. I have also reviewed bank records for Gold Depot and Newport Precious Metals that show large volumes of activity that are consistent with precious metal businesses. Due to the covert nature of this investigation, I have not interviewed the owners of Gold Depot and Newport Precious Metals to determine the nature of the transactions between the Tier-3 bank accounts and the precious metal wholesalers. However, based on the above, I believe that the funds from the tax fraud that have been laundered through Tier-1, Tier-2, and Tier-3 bank accounts appear to have been and are being used to purchase gold or other precious metals.

d. Although I do not know the disposition of any gold that may have been purchased, based on my training and experience, I believe that the purpose of the money laundering of the tax fraud proceeds is to ultimately convert the funds to cash, monetary instruments, or another form such as precious metals that are not traceable back to the tax fraud. Based on

my conversations with other law enforcement officers, I know that purchase of gold and precious metals with illicit funds is a common way for criminals to integrate their illicit proceeds. I also know that after gold and precious metals are purchased, they are resold at a higher price, kept as an investment, or transported out of the country.

e. Based on my training and experience, I know that fraudsters keep cash and monetary instruments from illicit proceeds secured in their home, in a security safe, and/or storage units, or separated among different locations used in the scheme. This is done to prevent law enforcement officers from seizing their illicit proceeds at one location.

f. For the above reasons, I believe the schemers appear to be buying gold from the illicit tax fraud funds that have been layered through Tier 2 and Tier 3 bank accounts.

F. Money Laundering Schemes Related to This Scheme

1. FBI health care money laundering sting investigation involving Gagik Airapetian ("SCHEMER#1")

45. On or about March 17, 2016, I met with FBI SA Mark Matsumura. SA Matsumura told me the following regarding his investigation into a money laundering sting operation conducted on Gagik Airapetian (SCHEMER#1), who as discussed below is believed to be a leader of this money laundering scheme.

46. In August 2008, FBI SA Christopher Watkins arrested an individual for his/her role in a health care fraud scheme, who later became a Confidential Human Source ("CHS1"). SA Matsumura subsequently learned that CHS1 had previously used SCHEMER#1 to launder proceeds from CHS1's multiple health care fraud entities.

47. SA Matsumura told me that he obtained an analysis from other FBI personnel of bank records that confirmed that CHS1 had used SCHEMER#1 to launder approximately over \$1 million in health care fraud proceeds related to CHS1's 2008 arrest.

48. CHS1 told SA Watkins that SCHEMER#1 laundered the health care fraud proceeds through multiple bank accounts controlled by SCHEMER#1.

49. Based on that information and other investigation, the FBI began a money laundering sting operation on SCHEMER#1.

50. In 2012, CHS1, acting at the direction of the FBI, met with SCHEMER#1. CHS1 asked SCHEMER#1 if SCHEMER#1 would be able to launder illicit proceeds for CHS1. When they spoke, they did not use the specific words that they would be laundering proceeds from "health care fraud," but, based on their prior interactions involving laundering proceeds from health care fraud, they both understood that the proceeds would be coming from health care fraud. SCHEMER#1 agreed to launder those proceeds for CHS1. From September 2012 through August 2013, SCHEMER#1 laundered approximately \$400,000 of FBI undercover

funds purported to be proceeds of health care fraud. SCHEMER#1 charged a money laundering fee of 30%.

51. SCHEMER#1 explained to CHS1 that he supervises the movement of money but that he did not physically do it himself.

52. Approximately 20 or more meetings were held at or around NS Wireless (SUBJECT PREMISES #2) where checks were being dropped off and/or cash was subsequently being picked up. There were some instances where checks were dropped off and cash was picked up during the same meeting.

53. SCHEMER#1's method of laundering health care fraud proceeds is similar to the method used to launder the proceeds from tax fraud. SA Matsumura traced the FBI funds that had been provided to SCHEMER#1 as part of the FBI sting operation. During the FBI sting operation, SCHEMER#1 used 24 checks to launder the funds and directed them to be deposited into 14 different bank accounts.

a. SA Matsumura confirmed that SCHEMER#1 laundered the FBI funds in the same way he had previously laundered the illegal proceeds for CHS1. That method was to provide SCHEMER#1 with signed blank checks from the bank account from which the illegal proceeds of health care fraud were drawn.

b. As part of the FBI sting operation of SCHEMER#1, CHS1 would specify the amount of funds to be laundered per instructions of his FBI handler. SCHEMER#1 would then direct the number of checks to deposit and set forth the bank accounts under his control into which the check(s) should be deposited.

SCHEMER#1 and/or someone else would fill out the amount and payees on these pre-signed checks.

c. SCHEMER#1 would then deduct his percentage for the laundering fee, and the balance would then be provided to CHS1 in cash a couple of weeks later.

d. On most occasions, the method of returning cash to CHS1 was secreting it inside a cell phone box, making it appear to be a cell phone transaction.

54. SCHEMER#1 used Non Stop Wireless (SUBJECT PREMISES #2) as a meeting place to launder FBI undercover sting money.

SCHEMER#1 directed CHS1 to bring the checks to, and/or pick up cash at or near, Non Stop Wireless aka "NS Wireless" (SUBJECT PREMISES #2), which is located as Unit A on 12901 Sherman Way in North Hollywood, California. Those surrounding locations also included a bus stop bench located on the NW corner of Coldwater Canyon and Sherman Way (which is northwest corner of Coldwater Canyon and Sherman Way adjacent to the strip mall in which NS Wireless is located), and the parking area on the north side of the Dunn Edwards paint store located on the NE corner of Coldwater Canyon and Sherman Way (located across the street from the aforementioned bench).

a. CHS1 would generally provide the checks to be laundered by SCHEMER#1 inside an envelope, and take them to SUBJECT PREMISES #2 to drop them off for SCHEMER#1.

b. CHS1 generally provided checks to be laundered to an individual later identified as Stepan Terakopyan. On one

occasion, CHS1 provided checks to Stepan Terakopyan without an envelope. The checks were displayed for Stepan Terakopyan to see. The checks were left at SUBJECT PREMISES #2.

55. SCHEMER#1 tells CHS1 that he is aware of IRS tax schemes. During a recorded meeting with CHS1, CHS1 asked SCHEMER#1 what he knew about taxes (referring to tax fraud), and SCHEMER#1 warned CHS1 that the "three letter ones" will be waiting to arrest you if you do that.

56. The first checks of the FBI sting operation were deposited into a Bank of America account in the name of "Arsen Aghayan." Analysis of that bank account shows deposits not only from the checks that were part of the FBI's sting operation, but also from a bank account in the name of "Armen Martirosyan" at First Citizens Bank in South Carolina. An analysis of that bank account showed that more than \$400,000 in likely fraudulently obtained IRS tax refunds were deposited into it.

57. SA Matsumura reviewed Aghayan's Bank of America records. Agents went to the address listed as the account of record and learned that it was a private mailbox. Agents asked for a copy of the rental application and identification that was provided to open the private mailbox. Within that application was a copy of the leasing application and an Armenian Passport in the name of "Arsen Aghayan." "Aghayan" was later identified to have the true name of Nikoghos Petrosyan.

58. As part of the FBI investigation in Seattle, Washington, discussed immediately following, it was uncovered

that Nikoghos Petrosyan opened approximately ten other bank accounts using other people's identities.

2. IRS-CI and FBI Seattle tax fraud investigation

59. I have spoken with IRS-CI SA Kendall McColley, who beginning in 2011 investigated a stolen identity and IRS refund theft crime ring in Seattle, Washington ("Seattle Investigation"). In addition to speaking with SA McColley, I also reviewed reports generated by the Seattle Investigation and learned that that scheme involved opening bank accounts under false names using altered Armenian passports. Those bank accounts were then used to receive direct deposits of tax refunds from federal tax returns filed in the names of real U.S. taxpayers whose identities had been stolen. Those refunds were paid as the result of false returns reporting wages from false Forms W-2 with inflated federal income tax withholding amounts.

60. The Seattle Investigation discovered approximately 4,500 tax returns filed in 2010 for tax year 2009, claiming refunds of approximately \$30,000,000. Approximately 5,500 tax returns were filed in 2011 for tax year 2010 claiming refunds of approximately \$35,000,000. It is estimated that the IRS paid out approximately one-third to one-half of those refund amounts.

61. The Seattle Investigation identified Nikoghos Petrosyan as one of several individuals who had used fraudulent passports to open bank accounts used in that scheme. Nikoghos Petrosyan opened several such bank accounts, including JPMorgan Chase account 931932545 in the name of "Eduard Karapetyan" and

another bank account in the name of "Aghasi Mkrtchyan" at JPMorgan Chase bank. In 2011, a check from JPMorgan Chase bank account 931932545 and a check in the name of Eduard Karapetyan were deposited to a bank account that was subsequently used as a Tier-2 bank account in the name of "Ashot Bekejyan" in this scheme. (As discussed below, SCHEMER#4 opened a bank account in the identity of "Ashot Bekejyan," which is not SCHEMER#4's true identity.)

62. The Seattle Investigation identified Gagik Airapetian (discussed below as SCHEMER#1), Mkhitar Mkrtchyan (discussed below as SCHEMER#11), Arman Abrahamyan (discussed below as SCHEMER#13), and Haroutioun Demirdjian (discussed below as SCHEMER#17) as being involved in the laundering of the money in their case. As discussed below, SCHEMER#1, SCHEMER#11, SCHEMER#13, and SCHEMER#16 are also involved in this scheme.

G. The Use of Private Mailboxes to Facilitate Money Laundering

63. I know that United States Postal Service Form 1583, "Application for Delivery of Mail Through Agent," is used when an individual applies to receive mail at a private mailbox located at a CMRA. I know that the application requires two types of identification to be provided, one of which must contain a photograph of the addressee.

64. During the course of this investigation, more than 200 private mailboxes have been identified as being used by the conspirators of this scheme to establish mailing addresses for the false identities that were then used to open bank accounts

used in this scheme. Other agents and I have interviewed employees or owners of these private mailbox services and obtained copies of the applications and identifications used to open these boxes. I have read the statements made by the owners and employees of the private mail services, and I have reviewed the applications provided by the private mail services. These owners and employees have either remembered the individuals who rented the boxes or stated that it is standard procedure to ensure that the identification match the individual who is applying to rent a mailbox, including comparing the picture on the proffered identification to the person who is attempting to rent the mailbox.

65. I have examined the photographic identifications from the files of the CMRAs, which were provided to the CMRAs when the schemers opened the mailboxes as part of the scheme. My review of those files show that the schemers discussed in depth in the following section, including Karen Pogolian (SCHEMER#2), Armen Mkrtchyan (SCHEMER#3), Sargis Tabadzhyan aka "Sergio Tabadzhyan" (SCHEMER#4), Hripsime Avagyan (SCHEMER#5), Jane Doe (SCHEMER#6), Artash Stepanyan (SCHEMER#7), Eduard Astvatsatryan (SCHEMER#8), John Doe (SCHEMER#9), Konstantin Galstyan (SCHEMER#10), and Mkhitar Mkrtchyan (SCHEMER#11), opened mailboxes using fraudulent identifications in identities that were not their own. The facts regarding these schemers, SCHEMER#2 to SCHEMER#11, inclusive, are discussed in detail in the next section, listed by respective schemer.

H. Identified Schemers in This Investigation

1. SCHEMER#1: Gagik Airapetian

66. Based on the investigation, I believe that Gagik Airapetian (SCHEMER#1) is the leader of this money laundering scheme. As discussed above, SCHEMER#1 operates the money laundering scheme by utilizing multiple bank accounts to layer illicit proceeds of tax refund fraud and other frauds. The proceeds are layered through at least two bank accounts before they are deposited into business bank accounts of purported Jewelry businesses located in downtown Los Angeles, California. Millions of dollars a year move through such bank accounts, making it difficult to trace.

67. SCHEMER#1 has been the target of multiple federal criminal investigations for money laundering, tax refund fraud, and health care fraud. Specifically, as discussed above, the FBI conducted a money laundering sting on SCHEMER#1 in 2012, wherein SCHEMER#1 laundered approximately \$400,000 in funds that he thought were proceeds of health care fraud. As detailed above, SCHEMER#1 used SUBJECT PREMISES #2 as part of that previous money laundering scheme.

68. As part of this money laundering scheme, SCHEMER#1 and his co-conspirators have utilized sophisticated techniques to disguise their illegal money laundering operations as legitimate transactions and to avoid detection from law enforcement. For example, SCHEMER#1 and/or his co-conspirators recruit other individuals, often who speak Armenian, to open bank accounts and

private mailboxes with fraudulent or altered passports from the countries of the Republic of Armenia, the country of Georgia, the Czech Republic, and other Eastern European countries. By having his co-conspirators use fraudulent or altered passports, SCHEMER#1 can launder money through the bank accounts that were opened, without the funds being tied to an actual person.

69. As discussed below, SCHEMER#1 has been observed at SUBJECT PREMISES #1 - the known hub of operations for this money laundering scheme - at least 22 times since August 3, 2015, and as recent as Friday, April 15, 2016. Every time that SCHEMER #1 was observed at SUBJECT PREMISES #1, at least one of the schemers known to have used other individuals' identities as part of the scheme was also present at SUBJECT PREMISES #1 with SCHEMER#1. As discussed below, on multiple occasions, SCHEMER#1 has been observed conversing with such schemers at SUBJECT PREMISES #1.

70. As discussed elsewhere in this Affidavit, SCHEMER#1 has been observed with known schemers at locations other than SUBJECT PREMISES #1, including SUBJECT PREMISES #2, and business Chic Accessories.

71. As discussed in depth below in the section focusing on SUBJECT PREMISES #1 and SUBJECT PREMISES #2, SCHEMER#1 has been observed travelling between those two locations used in this scheme, and directing and waiting at SUBJECT PREMISES #1 for the runners discussed below to return from conducting transactions in furtherance of this scheme.

72. As discussed in depth below in the section focusing on SUBJECT PREMISES #3 (SCHEMER#1's residence), SCHEMER#1 has been observed traveling with SUBJECT BAG #1 among the known scheme locations of SUBJECT PREMISES #1 and SUBJECT PREMISES #2 and SUBJECT PREMISES #3.

73. Thus, based on the investigation, and my training and experience, I believe that SCHEMER#1 is a leader of this money laundering scheme.

2. SCHEMER#2: Karen Pogolian

74. Based on the facts immediately following, I believe that Karen Pogolian (SCHEMER#2), posing and using fraudulent identifications in different identities that were not his true identity, rented at least two mailboxes and opened at least two bank accounts that were used in this scheme. Below are the details of the mailboxes and the bank accounts opened by SCHEMER#2, and the identifications in different identities that he used to do so.

75. On August 8, 2012, box #560 at Encino Mailboxes, 4924 Balboa Blvd., Encino, California, was rented in the name of "Hrachya Sevyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AM0330985 in the name of "Hrachya Sevyan" that had SCHEMER#2's photograph on it.

76. On December 11, 2013, box #501 at West Coast Mail Centers, 13659 Victory Blvd., Van Nuys, California, was rented in the name of "Ruben Pivazyan." When opening that mailbox, the

individual posing in that identity provided as identification Republic of Armenia passport number AH0638764 in the name of "Ruben Pivazyan" that had SCHEMER#2's photograph on it.

77. I have examined the photo identifications in the names of "Hrachya Sevyan" and "Ruben Pivazyan" that were used to open the mailboxes listed above, which I then compared to the photograph on the California driver's license issued to SCHEMER#2. I believe that the person depicted in the photo identifications used to open the two mailboxes in the different names listed above is actually SCHEMER#2.

78. The Republic of Armenia informed the U.S. Embassy in Armenia that passport number AM0330985 was issued in the name of "Hrachya Sevyan." Therefore I believe that passport number AM0330985 was altered to display SCHEMER#2's image and then used by SCHEMER#2 to rent a private mailbox as part of this scheme.

79. I have reviewed bank records of a bank account in the name of "Hrachya Sevyan," and believe that SCHEMER#2, posing in the identity of Hrachya Sevyan, opened a bank account that was used as a Tier-2 bank account in this scheme.

80. On August 31, 2012, Union Bank checking account 0030279026 and savings account 0030279034 were opened in the name of "Hrachya Sevyan." The address on the signature cards is "Melkonyan 2/3 #24, Yerevan, Armenia 0016." The address on the statements was initially listed as 5632 Van Nuys Blvd., #331, Van Nuys, California. However, with the statement beginning October 24, 2012, the address was listed as 4924 Balboa Blvd.,

Ste. 560, Encino, California. That address matches the first mailbox described above that was opened by SCHEMER#2.

a. Union Bank checking account 0030279026 operated as a Tier-2 bank account in 2013 and 2014, with deposits consisting of checks drawn on Tier-1 and Tier-2 bank accounts, and checks written from the account payable to LA Hoops and Unika Jewelry.

b. Union Bank savings account 0030279034 operated as a Tier-2 bank account in 2014, receiving one deposit from a check drawn from another Tier-2 bank account. The majority of the funds in this account were then transferred to checking account 0030279026.

81. In addition to the bank accounts discussed above, I have reviewed additional bank records that show there was at least one other bank account opened in the name of "Hrachya Sevyan."

82. I have reviewed bank records relating to "Ruben Pivzayan," and I believe that SCHEMER#2, posing in the identity of Ruben Pivzayan, opened two bank accounts that were used as Tier-2 bank accounts in this scheme, as described here:

a. On December 8, 2013, Wells Fargo Bank checking account 2609118050 and savings account 5608697743 were opened in the name of "Ruben Pivzayan" at a branch in Panorama City, California. The address on the signature card is listed as 13659 Victory Blvd., #501, Van Nuys, California, which is the second mailbox discussed above. The identification listed on

the signature card is Armenian passport number AH0638764, which is the same number as the Republic of Armenia passport used to open the mailbox discussed above.

b. Wells Fargo Bank checking account 2609118050 operated as a Tier-2 bank account in this scheme in 2014 with deposits consisting of checks drawn from other Tier-1 and Tier-2 bank accounts, and checks on the account made payable to Tier-2 and Tier-3 bank accounts, including to Zig Zag, LA Hoops, M&M Jewelry, and Moses Seraydaryan.

c. Wells Fargo Bank savings account 5608697743 operated as a Tier-2 bank account in this scheme in 2014, receiving deposits of checks drawn on Tier-1 bank accounts. The funds were then transferred to checking account 2609118050.

83. FBI SA Matsumura identified SCHEMER#2 as the person depicted in the passports in the names of "Ruben Pivzayan" and "Hrachya Sevyan" discussed above. I decided to interview SCHEMER#2 to see if he would cooperate and provide information relating to this scheme.

84. On October 23, 2015, HSI SA Michael Ou, Los Angeles Police Department Detective A. Mkrtchyan, and I interviewed SCHEMER#2.

a. SCHEMER#2 admitted that in 2012, 2013, and 2014, he opened several bank accounts and private mailboxes using fraudulent passports in other identities. SCHEMER#2 said that he was paid \$13,000 to \$14,000 for opening those bank accounts. He

also admitted depositing checks into other people's bank accounts.

b. SCHEMER#2 admitted that he knew it was illegal to open the bank accounts using the fraudulent identities and believes that the bank accounts he opened were used to launder money. SCHEMER#2 stated that he recalled using fraudulent passports in the names of "Hracha" and "Hakob."

c. SCHEMER#2 also said that in or around 2013 and possibly 2014, he used two or three other identities to open more bank accounts and private mailboxes, but that he could not recall the names he had used. SCHEMER#2 stated that using different identities, he opened bank accounts at Bank of America, Wells Fargo Bank, Union Bank, JPMorgan Chase, and possibly at Citibank. SCHEMER#2 also admitted that he would obtain a Costco membership card in the name of the identity he was assuming and present the Costco card to banks and CMRAs as a second form of identification.

d. SCHEMER#2 explained that he would provide a passport-sized photo of himself to his handler, who would then provide him with fraudulent passports that displayed his photo.

3. **SCHEMER#3: Armen Mkrtchyan**

85. Based on the facts immediately following, I believe that Armen Mkrtchyan (SCHEMER#3), posing and using fraudulent identification in identities that were not his true identity, rented at least two mailboxes used in the scheme. Below are the details of the mailboxes rented by SCHEMER#3 and the bank

accounts opened by SCHEMER#3, and the identifications in different identities that he used to do so.

86. On July 22, 2014, box #884 at the UPS Store Toluca Lake, 10061 Riverside Dr., Toluca Lake, California, was rented in the name of "Vahagn Vardanyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AM0617861 and Costco membership card number 11183690374, both in the name of "Vahagn Vardanyan." Both of those identification documents appear to have the photograph of SCHEMER#3.

87. On October 9, 2014, box #318 at the UPS Store #5626, 8309 Laurel Canyon Blvd., Sun Valley, California, was rented in the name of "Gagik Sargsyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0502118 and Costco membership card number 111838812692, both in the name of "Gagik Sargsyan." Both of those identification documents appear to have the photograph of SCHEMER#3.

88. I have examined the photo identifications in the names of "Vahagn Vardanyan" and "Gagik Sargsyan" that were used to open the mailboxes listed above, and I believe that not only are they the same person but that the passport photographs might actually be the same photograph. I then compared those photographs to the photograph on the California driver's license issued to SCHEMER#3, and based on that comparison, I believe that the person depicted in the photo identifications used to

open the two mailboxes in the different names listed above is actually SCHEMER#3.

89. I have reviewed bank records related to "Vahagn Vardanyan," and I believe that SCHEMER#3, using the identity of Vahagn Vardanyan, opened a bank account that was used as a Tier-2 bank account in this scheme, as described here:

a. On September 6, 2014, in Toluca Lake, California, JPMorgan Chase bank account 638937396 was opened in the name of "Vahagn Vardanyan." The identification listed on the signature card is Armenian passport AM0617861 (the same passport number used to open the first mailbox listed above). The address listed on the signature card is 10061 Riverside Dr., Apt. 884, Toluca Lake, California.

b. JPMorgan Chase bank account 638937396 operated as a Tier-2 bank account in 2015, with deposits consisting mostly of checks drawn from Tier-1 and Tier-2 bank accounts. Additionally, many checks drawn on the account were made payable to other Tier-2 bank account holders, as well as to Tier-3 bank account holders, including Unika Inc., Garo Minassian, HD Jewelry, and Zig Zag Jewelry.

c. In addition to the bank account above, I have reviewed bank records that show there was at least one other bank account opened in the name of Vahagn Vardanyan.

90. I have reviewed bank records related to "Gagik Sargsyan," and I believe that SCHEMER#3, posing in the identity

of Gagik Sargsyan, opened a bank account that was used as a Tier-2 bank account in this scheme, as described here:

a. On November 16, 2014, Bank of America account 325019792479 was opened in Sun Valley, California, in the name of Gagik Sargsyan Sole Prop DBA Sagigagi Jw. The identification on the signature card is listed as Armenian passport number AN0502118 (the same passport number used to open the second mailbox listed above), and the address as 8309 Laurel Canyon Blvd., #91, Sun Valley, California. Gagik Sargsyan is listed as the owner and sole signer on the account. The address on the statements is listed as 8309 Laurel Canyon Blvd. #139, Sun Valley, California, and the address on the checks is 8309 Laurel Canyon Blvd. #318, Sun Valley, California.

b. Bank of America account 325019792479 operated as a Tier-2 bank account in 2015 with deposits of checks drawn from other Tier-2 bank accounts. Checks drawn on the bank account were mostly made payable to Tier-3 bank accounts, including M & M, Seray Inc., and Zig Zag.

c. In addition to the bank account discussed above, I have reviewed additional bank records that show there was at least one other bank account opened in the name of "Gagik Sargsyan."

91. On August 19, 2015, I observed Harutyun Sukiasyan (described below as SCHEMER#14) driving a vehicle that was registered to SCHEMER#3. I obtained SCHEMER#3's California driver's license, and on a later date, I recognized the

photograph on that driver's license to be the same person in the photographs on the Vahagn Vardanyan and Gagik Sargsyan passports.

4. SCHEMER#4: Sargis Tabadzhyan, AKA "Sergio Tabadzhyan"

92. Based on the facts immediately following, I believe that Sargis Tabadzhyan (SCHEMER#4), posing and using fraudulent identification in different identities that were not his true identity, rented at least 7 mailboxes and opened 13 bank accounts that were used in this scheme. Below are the details of the mailboxes rented by SCHEMER#4 and the bank accounts opened by SCHEMER#4, and the identifications in different identities that he used to do so.

93. On August 24, 2010, box #222 at the Montebello UPS Store, 1012 W. Beverly Blvd., Montebello, California, was rented in the name of "Ashot Bekejyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AF0741659 in the name of "Ashot Bekejyan" that had SCHEMER#4's photograph on it.

94. On June 7, 2011, box #113 at CopyCat LA, 2046 Hillhurst Ave., Los Angeles, California, was rented in the name of "Khachatur Grigoryan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0630615 in the name of "Khachatur Grigoryan" that had SCHEMER#4's photograph on it.

95. On October 26, 2011, box #269 at Valley Mail, 11684 Ventura Blvd., Studio City, California, was rented in the name

of "Norayr Hakobyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0623757 in the name of "Norayr Hakobyan" that had SCHEMER#4's photograph on it.

96. On November 29, 2012, box #372 at West Coast Mail Center, 13659 Victory Blvd., Van Nuys, California, was rented in the name of "Rima Nersisyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AG0683232 in the name of "Rima Nersisyan" that had SCHEMER#4's photograph on it. That passport indicates that "Rima Nersisyan" is female, whereas SCHEMER#4 is actually male.

97. On August 8, 2013, box #428 at West Coast Mail Center, 13659 Victory Blvd., Van Nuys, California, was rented in the name of "Pogos Terakopyan." When opening that mailbox, the individual posing in that identity provided as identification California Identification Card number D1644041 in the name of "Pogos Terakopyan" that had SCHEMER#4's photograph on it.

a. I confirmed that California Identification Card number D1644041 was never issued by the State of California. Rather, number D1644041 was issued as a California driver's license to "Pogos Terakopyan," but the photograph of that individual does not resemble SCHEMER#4. (I subsequently discovered that Pogos Terakopyan is actually tied to the owners of NS Wireless (SUBJECT PREMISES #2), because the address for

California driver's license D1644041 is the same address listed for one of the owners of the business at SUBJECT PREMISES #2.)

98. On November 12, 2013, box #329 at the UPS Store, Montebello, 1012 W. Beverly Blvd., Montebello, California, was rented in the name of "Vaghinak Sosyan." When opening that mailbox, the individual posing in that name provided as identification Republic of Armenia passport number AH0296278 and Costco membership card number 111829717807, both in the name of "Vaghinak Sosyan." Both of those identification documents appear to have the photograph of SCHEMER#4. SCHEMER#4 also provided a Time Warner Cable bill for account number 6558552285286858 in the name of "Vaghinak Sosyan" with address 1765 Neil Armstrong St., Montebello, California.

99. On June 15, 2014, box #74 at Valley Postal, 300 W. Valley Blvd., Alhambra, California, was rented in the name of "Aram Hakobyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0506268 and Costco membership card number 111833814659, both in the name of "Aram Hakobyan." Both of those identification documents appear to have the photograph of SCHEMER#4.

100. I have examined the photo identifications used to open the seven private mailboxes discussed above, and I have compared those photo identifications to the California driver's license issued in the true name of SCHEMER#4. Based on those

comparisons, I believe the photographs are all of the same person, SCHEMER#4.

101. The Republic of Armenia informed the U.S. Embassy in Armenia that passports AF0741659, AH0630615, AG0683232, AH0296278, and AK0506268 were issued in the names of Ashot Bekejyan, Khachatur Grigoryan, Rima Nersisyan, Vaghinak Sosyan, and Aram Hakobyan, respectively. Therefore, I believe that Republic of Armenia passport numbers AF0741659, AH0630615, AG0683232, AH0296278, and AK0506268 were altered to display SCHEMER#4's image, and then used to rent private mailboxes.

102. SCHEMER#4 was also identified when retrieving mail at one of the mailbox locations, the UPS Store in Montebello, California:

a. On April 9, 2015, IRS SA Leonard observed an individual, whom he later identified as SCHEMER#4, exit the UPS Store in Montebello with an unknown male. When SA Leonard questioned the store employee who had assisted SCHEMER#4, the employee (Robert Alvarado) stated that the two males requested the mail for box #329, which had been opened in the name of "Vaghinak Sosyan." The male purporting to be "Vaghinak Sosyan" did not speak English and was assisted by the other male. Alvarado provided the mail for box #329 to the other male. SA Leonard identified SCHEMER#4 by obtaining the vehicle registration of the vehicle that SCHEMER#4 had used to depart the UPS store in Montebello. The vehicle was registered to SCHEMER#4, so SA Leonard obtained a copy of SCHEMER#4's

California driver's license, which is in his true name: Sergio Tabadzhyan AKA Sargis Tabadzhyan. SA Leonard determined that SCHEMER#4 was the same person who was at the UPS Store in Montebello on April 9, 2015, purporting to be "Vaghinak Sosyan."

b. On May 1, 2015, SA Leonard showed a photograph of SCHEMER#4 (from his California driver's license) to Alvarado. Alvarado identified SCHEMER#4 as the individual purporting to be "Vaghinak Sosyan" at the UPS Store-Montebello on April 9, 2015. He also recognized SCHEMER#4 as the same individual who had opened box 222 in the different name of "Ashot Bekejyan."

c. Alvarado also told SA Leonard that a female came in the store on April 30, 2015, and picked up mail from box #222, which consisted of two FedEx envelopes from Citibank. Alvarado described her as about 5'7" or 5'8" including high heels, slim build, and in her early to mid-twenties. The female had a mole above her upper lip and she spoke with an Eastern European accent. On May 1, 2015, SA Leonard emailed Alvarado four photographs provided by U.S. Bank of a female with a mole who had transacted on the U.S. Bank account of "Manvel Sargsyan." On May 8, 2015, SA Leonard spoke with Alvarado who identified the female in the four photographs as the female who had been in the store on April 30, 2015, to pick up mail. I have examined the four photographs, and I believe that the female in those photographs is Hripsime Avagyan (SCHEMER#5 below).

103. I have reviewed bank records for "Rima Nersisyan," and I believe that SCHEMER#4, using the identity of Rima Nersisyan, opened two bank accounts that were used as Tier-1 bank accounts in this scheme, as described here:

a. On December 3, 2012, in Burbank, California, Wells Fargo Bank checking account 6978755814 and savings account 7094298929 were opened in the name of "Rima Nersisyan." The customer residence is listed as 13659 Victory Blvd #372, Van Nuys, California, and the identification as Armenian passport AG0683232 (the same passport number used to open one of the mailboxes listed above).

b. The review of the records also shows that bank account 6978755814 received two electronic deposits of fraudulently obtained tax refunds from the IRS on February 11, 2014, and March 12, 2014, totaling \$11,404. Records also show that account number 7094298929 received three electronic deposits of fraudulently obtained tax refunds from the IRS on February 11, 2014, February 12, 2014, and March 10, 2014, totaling \$20,497.

c. In addition to the bank accounts above, I have reviewed additional bank records that show there were at least three other bank accounts opened in the name of "Rima Nersisyan."

104. I have reviewed bank records for "Ashot Bekejyan," and I believe that SCHEMER#4, posing in the identity of Ashot

Bekejyan, opened a bank account that was used as a Tier-2 bank account in this scheme, as described here:

a. On September 25, 2010, Wells Fargo Bank account 9855513157 was opened in Montebello, California, in the name of "Ashot Bekejyan." The address listed on the signature card is 1012 W. Beverly Blvd., Apt. 222, Montebello, California, and the identification is listed as Armenian passport AF0741659 (the same passport number used to open the first mailbox listed above).

b. Wells Fargo Bank account 9855513157 operated as a Tier-2 bank account in 2012, 2013, and 2014. Deposits to that bank account in 2012, 2013, and 2014 consist mostly of checks drawn from Tier-1 and Tier-2 bank accounts, and the withdrawals mostly consist of checks made payable to Tier-2 and Tier-3 bank accounts, including to HD Jewelry, Zig Zag, Unika Jewelry, LA Hoops, and Garo Minassian.

c. Additionally, deposits to bank account 9855513157 in 2011 include checks from two individuals, "Eduard Karapetyan" and "Aghasi Mkrtchyan," which names were both known to the Seattle Investigation, but which are really just one person whose true identity is Nikoghos Petrosyan. The check from "Eduard Karapetyan" was drawn on an account identified in the Seattle investigation as being opened by Nikoghos Petrosyan on November 27, 2010, in Northridge, California. Electronic payments from account 9855513157 also include payments on credit card accounts in the name of Stepan Terakopyan. Both Stepan

Terakopyan (discussed below as an owner/operator of the business at SUBJECT PREMISES #2) and Nikoghos Petrosyan were also involved in the FBI investigation.

d. In addition to the bank account above, I have reviewed additional bank records that show there were at least 11 other bank accounts opened in the name of "Ashot Bekejyan."

105. I have reviewed bank records for "Vaghinak Sosyan," and I believe that SCHEMER#4 opened bank accounts in the name of Vaghinak Sosyan that were used as Tier-2 bank accounts in this scheme, as described here:

a. On December 13, 2013, Citibank bank accounts 42010620666 and 42010620674 were opened in the name of "Vaghinak Sosyan." Account 42010620666 was a checking account, and 42010620674 was a savings account. The address listed on the signature card is 1765 Neil Armstrong, Apt. #204, Montebello, California. The address on the statements is initially the same as that listed on the signature card; however, beginning with the statement dated March 16 through April 2015, the address is listed as 1012 W. Beverly Blvd., Apt. 329, Montebello, California.

b. Citibank bank accounts 42010620666 and 42010620674 operated as Tier-2 bank accounts in 2014 and 2015. Deposits to the bank accounts consist mostly of checks drawn on Tier-1 and Tier-2 bank accounts. Additionally, multiple checks were drawn on bank account 42010620666 payable to other Tier-2

bank account holders, as well as to Tier-3 bank account holders, including Unika Inc., L.A. Hoops, M&M Jewelry, and HD Jewelry.

c. In addition to the bank accounts above, I have reviewed additional bank records that show there were at least five other bank accounts opened in the name of "Vaghinak Sosyan."

106. I have also reviewed additional bank records that show there were at least:

a. two bank accounts opened in the name of "Khachatur Grigoryan;"

b. two bank accounts opened in the name of "Norayr Hakobyan;" and

c. three bank accounts opened in the name of "Aram Hakobyan."

5. **SCHEMER#5: Hripsime Avagyan**

107. Based on the facts immediately following, I believe that Hripsime Avagyan (SCHEMER#5), posing and using fraudulent identification in different identities that were not her true identity, rented at least 7 mailboxes and opened at least 6 bank accounts that were used in this scheme. Below are the details of the mailboxes rented by SCHEMER#5 and the bank accounts opened by SCHEMER#5, and the identifications in different identities that she used to do so.

108. On November 19, 2013, box #389 at Beverly Mailbox Rentals, 326 N. Western Ave., Los Angeles, California, was rented in the name of "Tatevik Hunanyan." When opening that

mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0433907 and Costco membership card number 111829922843, both in the name of "Tatevik Hunanyan." Both of those identification documents appear to have the photograph of SCHEMER#5.

109. On November 21, 2013, box #152 at C&E Mailboxes, 5082 W. Pico, Los Angeles, California, was rented in the name of "Tehmine Khachatryan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0583579 and Costco membership card number 111829926152, both in the name of "Tehmine Khachatryan." Both of those identification documents appear to have the photograph of SCHEMER#5.

110. On December 3, 2013, box #476 at West Coast Mail Centers, 13659 Victory Blvd., Van Nuys, California, was rented in the name of "Lusin Alaverdyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AM0518750 and Costco membership card number 111830270349, both in the name of "Lusin Alaverdyan." Both of those identification documents appear to have the photograph of SCHEMER#5.

111. On April 4, 2014, two mailboxes at two different locations, in two different identities, were rented, neither of which was in SCHEMER#5's true identity.

a. On April 4, 2014, box #234 at Printing Zone Inc., 22815 Ventura Blvd., Woodland Hills, California, was rented in

the name of "Anna Harutyunyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AG0547511 and Costco membership card number 111833343191, both in the name of "Anna Harutyunyan." Both of those identification documents appear to have the photograph of SCHEMER#5.

b. On April 4, 2014, box #276 at Mailboxes N More, 25379 Wayne Mills Pl., Valencia, California, was rented in the name of "Anush Karapetyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AG0412836 that had SCHEMER#5's photograph on it.

112. On April 17, 2014, box #297 at Mail Plus, 269 S. Western Ave., Los Angeles, California, was rented in the name of "Ani Nahapetyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0526282 in the name of "Ani Nahapetyan" that had SCHEMER#5's photograph on it.

113. On April 18, 2014, box #223 at San Marino Mailbox, 1613 Chelsea Rd., San Marino, California, was rented in the name of "Ani Gevorgyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0260303 and Costco membership card number 111833846502, both in the name of "Ani Gevorgyan." Both of those identification documents appear to have the photograph of SCHEMER#5.

114. I have examined the photo identifications used to open the seven private mailboxes discussed above, and I have compared those photo identifications to the California driver's license issued in the true name of SCHEMER#5. I also examined the Republic of Armenia passport in SCHEMER#5's immigration records. Based on those comparisons, I believe the photographs are all of the same person, SCHEMER#5.

115. The Republic of Armenia informed the U.S. Embassy in Armenia that passport numbers AH0583579 and AM0518750 were issued in the names of Tehmine Khachatryan and Lusine Alaverdyan at one point in time, respectively. Therefore, I believe that Republic of Armenia passports AH0583579 and AM0518750 were altered to display SCHEMER#5's image and then used to rent private mailboxes.

116. I have reviewed bank records for "Tehmine Khachatryan," and I believe that SCHEMER#5, posing in the identity of Tehmine Khachatryan, opened a bank account that was used as a Tier-2 bank account in this scheme, as described here:

a. On January 13, 2014, Citibank account 42011010313 was opened in Los Angeles, California, in the name of "Tehmine Khachatryan." The identification documented on the account opening document was Armenian passport AH0583579 (the same passport number used to open the second mailbox listed above). The address listed on the statements is 5082 W. Pico, Apt. 512, Los Angeles, California. (I believe "512" resulted from

accidentally transposing "152," which was the corresponding mailbox that SCHEMER#5 had opened.)

b. Citibank account 42011010313 operated as a Tier-2 bank account in 2014 with deposits mostly consisting of checks drawn from Tier-1 and Tier-2 bank accounts. Withdrawals consisted mostly of checks made payable to Tier-2 and Tier-3 bank account holders, including Garo Minassian, HD Jewelry, LA Hoops, Unika Inc., and M&M Jewelry.

c. In addition to the bank accounts above, I have reviewed additional bank records that show there were at least five other bank accounts opened in the name of "Tehmine Khachatryan."

117. I have reviewed bank records for "Lusine Alaverdyan," and I believe that SCHEMER#5, posing in the identity of Lusine Alaverdyan, opened two bank accounts that were used as Tier-2 bank accounts in this scheme, as described here:

a. On January 13, 2014, Citibank bank accounts 42011055318 and 42011055300 were opened in Van Nuys, California, in the name of "Lusine Alaverdyan." The identification listed on one of the account opening documents is Armenian passport AM0518750 (the same passport number used to open the third mailbox listed above), and the address as 13659 Victory Blvd., Apt. 476, Van Nuys, California.

b. Citibank checking account 42011055300 and savings account 42011055318 operated as Tier-2 bank accounts in 2014, with deposits mostly consisting of checks drawn on Tier-1 and

Tier-2 bank accounts. Withdrawals consisted mostly of checks made payable from bank account 42011055300 to Tier-2 and Tier-3 bank account holders, including Garo Minassian, HD Jewelry, LA Hoops, Unika Inc., Zig Zag Jewelry, and M&M Jewelry.

c. In addition to the bank accounts above, I have reviewed additional bank records that show there were at least three other bank accounts opened in the name of "Lusine Alaverdyan."

118. I have also reviewed additional bank records that show there were at least:

- a. two bank accounts opened in the name "Tatevik Hunanyan;"
- b. three bank accounts opened in the name of "Anna Harutyunyan;"
- c. one bank account opened in the name of "Anush Karapetyan;" and
- d. one bank account opened in the name of "Ani Nahapetyan."

6. SCHEMER#6: Jane Doe

119. Based on the facts immediately following, I believe that "Jane Doe" (SCHEMER#6), a female whose true name we have not yet been able to identify, posing and using fraudulent identification in different identities, rented at least 6 mailboxes and opened 8 bank accounts that were used in this scheme. Below are the details of the mailboxes rented by

SCHEMER#6 and the bank accounts opened by SCHEMER#6, and the identifications in different identities that she used to do so.

120. On June 17, 2014, box #193 at Mailboxes Lido, 3419 Via Lido, Newport Beach, California, was rented in the name of "Nune Zakaryan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0627716 and Costco membership card number 111835441715, both in the name of "Nune Zakaryan." Both of those identification documents appear to have the photograph of SCHEMER#6.

121. On June 19, 2014, box #44 at AIM Mail Center, 10073 Valley View St., Cypress, California, was rented in the name of "Sirvard Khachatryan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0305054 in the name of "Sirvard Khachatryan" that had SCHEMER#6's photograph on it.

122. On June 20, 2014, box #203 at the UPS Store, 10910 Long Beach Blvd., Suite 103, Lynwood, California, was rented in the name of "Anahit Israelyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0727525 in the name of "Anahit Israelyan" that had SCHEMER#6's photograph on it. SCHEMER#6 also provided an AT&T Monthly Statement in the name of "Anahit Israelyan," which appears to be altered.

123. On June 23, 2014, box #216 at the Mail Depot, 401 S. Harbor Blvd., Ste. F, La Habra, California, was rented in the

name of "Hasmik Gasparyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0625238 in the name of "Hasmik Gasparyan" that had SCHEMER#6's photograph on it.

124. On May 28, 2015, box #858 at the UPS Store 0944, 1107 Fair Oaks Ave., South Pasadena, California, was rented in the name of "Elena Oganessian." When opening that mailbox, the individual posing in that identity provided as identification a country of Georgia passport number 05AA51086 and Costco membership card number 111845465024, both in the name of "Elena Oganessian." Both of those identification documents appear to have the photograph of SCHEMER#6.

125. On June 11, 2015, box #257 at the Printing Zone, 22815 Ventura Blvd., Woodland Hills, California, was rented in the name of "Iveta Mkrtchyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0690421 that had SCHEMER#6's photograph on it.

126. I have examined and compared the photo identifications in the names of Nune Zakaryan, Sirvard Khachatryan, Anahit Israelyan, Hasmik Gasparyan, Elena Oganessian, and Iveta Mkrtchyan, which were used to open the mailboxes listed above. Based on those comparisons, I believe the photographs are all of the same person, Jane Doe/SCHEMER#6.

127. On January 7, 2016, I observed SCHEMER#5 and SCHEMER#6 enter an East West Bank branch located at 135 N. Los Robles

Ave., Pasadena, California. I have reviewed photographs which confirmed that SCHEMER#6 and SCHEMER#5 were in the East West Bank on January 7, 2016. I was later informed by a bank employee that the person she knew as "Elena Oganessian" requested that her address be changed for her bank accounts. I therefore believe that while at the East West Bank on January 7, 2016, SCHEMER#6 represented herself as "Elena Oganessian," the name listed on accounts 178365565 and 2088014440 at East West Bank.

128. I have reviewed East West Bank records related to bank account numbers 178365565 and 2088014440. After reviewing the records, I confirmed that the account was opened in the name of "Elena Oganessian" on August 7, 2015, in Pasadena, California. The address on the signature card is listed as 1107 Fair Oaks Ave., South Pasadena, California. On January 7, 2016, SCHEMER#6 changed the address on the bank accounts to 1107 Fair Oaks Ave. #859, South Pasadena, California. Another bank employee later told me that the address was changed again on February 9, 2016, to 1107 Fair Oaks Ave. #858, South Pasadena, California.

129. I have also reviewed Bank of America records related to bank accounts opened in the name of "Elena Oganessian." In addition to bank records, I was provided with Bank of America ATM photos of account opening deposits on May 28, 2015. The ATM photos depict the individual I recognize as SCHEMER#6 depositing cash into accounts 325046641904 and 325057797944. Therefore, I believe that SCHEMER#6, posing in the identity of "Elena Oganessian," opened these bank accounts. The ATM photos also

show a female standing next to SCHEMER#6. I have examined these photographs and believe that that female is SCHEMER#5.

130. IA Gilmore told me that Bank of America accounts 325046641904 and 325057797944 had two tax refunds deposited into each account in 2016. I confirmed that each tax refund deposited was in the name of different individuals, neither of which is in the name of "Elena Oganessian."

131. I have also reviewed additional bank records that show there were at least:

a. four bank accounts opened in the name of "Nune Zakaryan;"

b. three bank accounts opened in the name of "Sirvard Khachatryan;"

c. two bank accounts opened in the name of "Anahit Israelyan;" and

d. three bank accounts opened in the name of "Hasmik Gasparyan."

7. SCHEMER#7: Artash Stepanyan

132. Based on the facts immediately following, I believe that Artash Stepanyan (SCHEMER#7), posing and using fraudulent identification in different identities that were not his true identity, rented at least 6 mailboxes and opened at least 14 bank accounts that were used in this scheme. Below are the details of the mailboxes rented by SCHEMER#7 and the bank accounts opened by SCHEMER#7, and the identifications in different identities that he used to do so.

133. On June 2, 2011, box #652 at Sunset Blvd. Mailboxes, 7119 W. Sunset Blvd., Los Angeles, California, was rented in the name of "Arman Asasyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0285765 in the name of "Arman Asasyan" that had SCHEMER#7's photograph on it.

134. On September 5, 2012, box #287 at Postalworks, 2658 Griffith Park Blvd, Los Angeles, California, was rented in the name of "Hamlet Muradyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AG0575869 in the name of "Hamlet Muradyan" that had SCHEMER#7's photograph on it.

135. On September 6, 2012, box #405 at UPS Store 1062, 9018 Balboa Blvd., Northridge, California, was rented in the name of "Artur Poghosyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0386504 in the name of "Artur Poghosyan" that had SCHEMER#7's photograph on it.

136. On June 26, 2013, box #347 at Mail Fax Plus USA, 11100-8 Sepulveda Blvd., Mission Hills, California, was rented in the name of "Manvel Sargsyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0386504 and Costco membership card number 111825203611, both in the name of "Manvel Sargsyan." However, the owner of Mail Fax Plus USA failed to keep copies of those identification items, even though

required to do so under U.S. postal regulations, so those numbers were just recorded in the file for the mailbox (as opposed to copies of the documents, like the other mailbox locations discussed in this Affidavit). To compare photographs, I obtained and served a federal Grand Jury subpoena on Costco for a copy of the photograph for Costco membership card 111825203611 in the name of Manvel Sargsyan, which Costco then provided. I then examined the photograph provided by Costco for Costco membership card number 111825203611, and I believe the person in that photograph is SCHEMER#7.

137. On September 16, 2013, box #328 at Cerritos Mailbox and More, 11432 South St., Cerritos, California, was rented in the name of "Hamlet Petrosyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AF0343649 and Costco membership card number 11828097528, both in the name of "Hamlet Petrosyan." Both of those identification documents appear to have the photograph of SCHEMER#7.

138. On October 4, 2013, box #81 at Torrance Postal N Shipping, 2100 Redondo Beach Blvd., Ste. C, Torrance, California, was rented in the name of "Artur Virabyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AG0393912 in the name of "Artur Virabyan" that had SCHEMER#7's photograph on it.

139. I examined the photograph identifications that were used to rent the six mailboxes described above, and I have compared them to the California driver's license issued to SCHEMER#7. Based on those comparisons, I believe the photographs are all of the same person, SCHEMER#7.

140. The Republic of Armenia informed the U.S. Embassy in Armenia that passports AG0393912, AK0285765, AK0386504, AF0343649, and AF0467653 were issued in the names of Artur Virabyan, Arman Asasyan, Artur Poghosyan, Hamlet Petrosyan, and Manvel Sargsyan, respectively. Therefore, I believe that the passports AG0393912, AK0285765, AK0386504, AF0343649, and AF0467653 were altered to display SCHEMER#7's image and then used to rent mailboxes as part of this scheme.

141. I have reviewed bank records for "Manvel Sargsyan," and I believe that SCHEMER#7, posing in the identity of Manvel Sargsyan, opened three bank accounts that were used as Tier-2 bank accounts in this scheme, as described here:

a. On September 9, 2013, U.S. Bank accounts 157502048133 and 253462993192 were opened in the name of "Manvel Sargsyan." The address on the signature card is 11100-8 Sepulveda Blvd #347, Mission Hills, California, and the identification provided was Armenian passport A50467653.

i. On or about August 26, 2014, I spoke with the U.S. Bank personal banker who opened accounts 157502048133 and 253462993192. The banker recognized the person on Costco

membership card 111825203611 in the name of "Manvel Sargsyan" as the person who had opened the account.

ii. U.S. Bank accounts 157502048133 and 253462993192 operated as Tier-2 bank accounts in this scheme in 2013 and 2014, receiving deposits of checks drawn from Tier-1 and other Tier-2 bank accounts. Funds from account 253462993192 were mostly transferred to 157502048133. Checks were drawn on account 157502048133 made payable to Tier-3 bank accounts, including LA Hoops and Unika Jewelry.

b. On June 26, 2013, Wells Fargo bank account 1058185032 was opened in the name of "Manvel Sargsyan." The address on the signature card is 11100 Sepulveda Blvd., Unit 347, Mission Hills, California, and the primary identification is listed as Armenian passport AF0467653 (the same passport number used to open one of the mailboxes listed above) and secondary identification as Costco membership card 111825203611 (the same Costco membership number used to open one of the mailboxes listed above).

i. Wells Fargo bank account 1058185032 operated as a Tier-2 bank account in this scheme in 2013 and 2014, receiving deposits of checks drawn from Tier-1 and other Tier-2 bank accounts. Checks were drawn on account 1058185032 made payable to Tier-2 and Tier-3 bank accounts, including LA Hoops, Unika Jewelry, and Zig Zag Jewelry.

ii. On December 30, 2014, SA Ou and I spoke with the Wells Fargo Bank personal banker who had closed the accounts

in the name of "Manvel Sargsyan." A photograph of SCHEMER#7 was provided to the personal banker, and the personal banker told us that he recognized SCHEMER#7 as the individual he knew as "Manvel Sargsyan." The banker said that SCHEMER#7 had entered the bank alone and presented an Armenian passport in the name of "Manvel Sargsyan." Approximately \$29,000 in cash from the "Manvel Sargsyan" bank account was released to SCHEMER#7.

142. In addition to the bank accounts described above, I have reviewed additional bank records that show there were at least three other bank accounts opened in the name in the name of "Manvel Sargsyan."

143. I have also reviewed additional bank records that show there were at least:

- a. four bank accounts opened in the name of "Arman Asasyan;"
- b. five bank accounts opened in the name of "Hamlet Muradyan;"
- c. six bank accounts opened in the name of "Hamlet Petrosyan;"
- d. nine bank accounts opened in the name of "Artur Virabyan;" and
- e. four bank accounts opened in the name of "Artur Poghosyan."

144. I have reviewed photographs provided by U.S. Bank that show a female and a male transacting on U.S. Bank account 157502048133. The female is shown transacting on the account on

February 11, 2014, February 13, 2014, February 14, 2014, February 27, 2014, and February 28 2014. I have examined these photographs, and based on the investigation, I believe that the female transacting on the accounts is SCHEMER#5. The male is shown transacting on the account on February 13, 2014, February 21, 2014, February 24, 2014, February 25, 2014, and February 26 2014. I have examined these photographs, and based on the investigation, I believe that the male transacting on those accounts is SCHEMER#17.

8. SCHEMER#8: Eduard Astvatsatryan

145. Based on the facts immediately following, I believe that Eduard Astvatsatryan (SCHEMER#8), posing and using fraudulent identification in different identities that were not his true identity, rented at least 14 mailboxes and opened at least 17 bank accounts that were used in this scheme. Below are the details of the mailboxes rented by SCHEMER#8 and the bank accounts opened by SCHEMER#8, and the identifications in different identities that she used to do so.

146. On May 15, 2014, box #333 at PakMail, 527 N. Azusa Ave., Covina, California, was rented in the name of "Hrant Abovyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AM0874122 and Costco membership card number 111834611391, both in the name of "Hrant Abovyan." Both of those identification documents appear to have the photograph of SCHEMER#8.

147. On May 15, 2014, box #262 at Mail Boxes Exp., 425 E. Arrow Highway, Glendora, California, was rented in the name of "Aram Vardanyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0328543 in the name of "Aram Vardanyan" that had SCHEMER#8's photograph on it.

148. On June 6, 2014, box #103 at the UPS Store #5406, 1004 West Covina Parkway, West Covina, California, was rented in the name of "Henrik Karapetyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AM0509129 and Costco membership card number 111835153802, both in the name of "Henrik Karapetyan." Both of those identification documents appear to have the photograph of SCHEMER#8.

149. On June 6, 2014, box #19 at Mail On The Go, 960 E. Alostia, Azusa, California, was rented in the name of "Khachatur Khachatryan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0415560 in the name of "Khachatur Khachatryan" that had SCHEMER#8's photograph on it.

150. On August 1, 2014, box #824 at the At Mail Store Inc., 17360 Colima Rd., Rowland Heights, California, was rented in the name of "Albert Askanazyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0230961 and Costco membership card number 111836369344, both in the name of "Albert

Askanazyan." Both of those identification documents appear to have the photograph of SCHEMER#8.

151. On August 4, 2014, box #354 at Mailboxes N More, 25379 Wayne Mills Rd., Valencia, California, was rented in the name of "Hovhannes Karapetyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AM0729400 in the name of "Hovhannes Karapetyan" that had SCHEMER#8's photograph on it.

152. On September 30, 2014, box #159 at All in One Mail Center, 10929 Firestone Blvd., Norwalk, California, was rented in the name of "Martin Sidelka." When opening that mailbox, the individual posing in that identity provided as identification Czech Republic passport number 12492971 in the name of "Martin Sidelka" that had SCHEMER#8's photograph on it.

153. On October 1, 2014, box #152 at Encino Mail Boxes, 4924 Balboa Blvd., Encino, California, was rented in the name of "Arman Saghatelyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0401444 in the name of "Arman Saghatelyan" that had SCHEMER#8's photograph on it.

154. On February 5, 2015, box #334 at S 'N' S Postal Center, 5917 Oak Ave., Temple City, California, was rented in the name of "Gegham Mkhitarian." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0676992 in the name of "Gegham Mkhitarian" that had SCHEMER#8's photograph on it.

155. On February 17, 2015, box #181 at Rapid Pak & Ship, 8860 Corbin Ave., Northridge, California, was rented in the name of "Armen Poghosyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0595699 in the name of "Armen Poghosyan" that had SCHEMER#8's photograph on it.

156. On February 18, 2015, box #335 at PostalAnnex #170, 5737 Kanan Rd., Agoura Hills, California, was rented in the name of "Sargis Manukyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0487773 in the name of "Sargis Manukyan" that had SCHEMER#8's photograph on it.

157. On February 19, 2015, box #941 at Hollywood Mail and Message Service, 1626 N. Wilcox Ave., Los Angeles, California, was rented in the name of "Arshak Khachatryan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AF0551561 in the name of "Arshak Khachatryan" that had SCHEMER#8's photograph on it.

158. On January 27, 2016, box #308 at Boxes and More, 8491 Sunset Blvd., West Hollywood, California, was rented in the name of "Edik Nasirov." When opening that mailbox, the individual posing in that identity provided as identification a country of Georgia passport number 05AB12642 in the name of "Edik Nasirov" that had SCHEMER#8's photograph on it.

159. On January 30, 2016, box #557 at Mailbox Services Plus, 14431 Ventura Blvd., Sherman Oaks, California, was rented in the name of "Mamikon Zeynalyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AN0380788 in the name of "Mamikon Zeynalyan" that had SCHEMER#8's photograph on it.

160. I examined the photograph identifications that were used to rent the mailboxes described above, and I have compared them to an international driver's license (number MWL1979514965), a Kazakhstan passport (N07350477), and a United States Visa (number 20131223440009), which were all issued to SCHEMER#8 in his true identity. Based on those comparisons, I believe the photographs are all of the same person, SCHEMER#8.

161. Additionally, I observed SCHEMER#8 enter Boxes and More, the CMRA located at 8491 Sunset Blvd., West Hollywood, California, on the day that box #308 was rented in the name of "Edik Nasirov." I spoke with the manager who identified SCHEMER#8 from SCHEMER#8's international driver's license (number MWL1979514965) as the individual who had just opened box #308 there.

162. The Republic of Armenia informed the U.S. Embassy in Armenia that passports AM0874122, AM0509129, AN0415560 and AN0595699 were issued in the names of Hrant Abovyan, Henrik Karapetyan, Khachatur Khachatryan, and Armen Poghosyan, respectively. Therefore I believe that Republic of Armenia

passports AM0874122, AM0509129, AN0415560, and AN0595699 were altered to display SCHEMER#8's image, and then used to rent mailboxes as part of this scheme.

163. I have reviewed bank records for "Hrant Abovyan," and I believe that SCHEMER#8, posing in the identity of Hrant Abovyan, opened a bank account that operated as a Tier-2 bank account in this scheme as described here:

a. On June 10, 2014, Citibank checking account 42013022753 and savings account 42013022761 were opened. The name and address on the bank statements are "Hrant Abovyan," 527 N. Azusa, #333, Covina, California.

b. Citibank accounts 42013022753 and 42013022761 operated as Tier-2 bank accounts in this scheme during 2015. Deposits consist mostly of checks drawn from Tier-1 and Tier-2 bank accounts. Withdrawals consisted mostly of checks payable from account 42013022753 to Tier-3 bank account holders, including Unika Inc. and HD Jewelry. Funds were withdrawn from account 42013022761 by transfers to account 42013022753.

164. In addition to the bank accounts above, I have reviewed additional bank records that show there were at least three other accounts opened in the name of "Hrant Abovyan."

165. I have also reviewed additional bank records that show there were also at least:

a. two bank accounts opened in the name of "Aram Vardanyan;"

- b. three bank accounts opened in the name of "Henrik Karapetyan;"
- c. three bank accounts opened in the name of "Khachatur Khachatryan;"
- d. four bank accounts opened in the name of "Albert Askanazyan;"
- e. two bank accounts opened in the name of "Martin Sidelka;"
- f. one bank account opened in the name of "Arman Saghatelyan;"
- g. two bank accounts opened in the name of "Gegham Mkhitaryan;"
- h. two bank accounts opened in the name of "Armen Poghosyan;"
- i. three bank accounts opened in the name of "Sargis Manukyan;" and
- j. two bank accounts opened in the name of "Arshak Khachatryan."

9. SCHEMER#9: John Doe

166. Based on the facts immediately following, I believe that "John Doe" (SCHEMER#9), a male whose true name we have not yet been able to identify, posing and using fraudulent identification in different identities, rented at least two mailboxes and opened four bank accounts in 2016. Below are the details of the mailboxes rented by SCHEMER#9 and the bank accounts opened by SCHEMER#9, and the identifications in

different identities that he used to do so.

167. On January 8, 2016, box #179 at Mailbox Plus, 5404 Whitsett Ave., Valley Village, California, was rented in the name of "Nugzar Arutinov." When opening that mailbox, the individual posing in that identity provided as identification a country of Georgia passport number 07AF57135 in the name of "Nugzar Arutinov" that had SCHEMER#9's photograph on it.

168. On January 11, 2016, box #535 at Mailbox Services Plus, 14431 Ventura Blvd., Sherman Oaks, California, was rented in the name of "Emzar Tsenteradze." When opening that mailbox, the individual posing in that identity provided as identification a country of Georgia passport number 05AA534964 in the name of "Emzar Tsenteradze" that had SCHEMER#9's photograph on it.

169. I have examined the photo identifications in the names of Nugzar Arutinov and Emzar Tsenteradze, and I believe that they are the same person, SCHEMER#9.

170. I have reviewed bank records for "Nugzar Arutinov," and I believe that SCHEMER#9, posing in the identity of Nugzar Arutinov, opened four bank accounts used in this scheme, as described here:

a. On January 27, 2016, in Hollywood, California, four Bank of America accounts were opened. Two of these accounts, 325060260646 and 325070141373, were business accounts opened in the name of "Nugzar Arutinov DBA Lotex." The identification listed on the signature cards is Georgian

passport number 07AF57135 (the same passport number used by SCHEMER#9 to open the mailbox in the name of "Nugzar Arutinov"). The bank statements for these two accounts are addressed to 5404 Whitsett Ave., Valley Village, California. Two of these accounts, 325070142123 and 325070142152, were personal accounts opened in the name of "Nugzar Arutinov." The identification listed on the signature cards is foreign passport 07AF57135 (the same passport used to open the first mailbox discussed above). The bank statements for account 325070142123 are addressed to 5404 Whitsett Ave. 179, Valley Village, California.

171. March 29, 2016:

a. On March 29, 2016, a Bank of America investigator notified me that "Nugzar Arutinov" had called the Hollywood Branch located at 7800 W. Sunset Blvd., Los Angeles, California, informing them that he would be at the bank in 30 minutes to order checks and turn in his Form W-8.

b. IRS SA Leonard and I went to the bank branch listed above to attempt to identify the identity of the individual posing as "Nugzar Arutinov." SA Leonard observed SCHEMER#9 speaking with a bank employee there. (Subsequently, I confirmed with a bank employee that SCHEMER#9 had posed in the identity of "Nugzar Arutinov," and ordered checks for the bank account in that name.)

c. SA Leonard followed SCHEMER#9 out of the bank, and SA Leonard and I observed SCHEMER#9 entering a vehicle and drive to the vicinity of the Avalon Apartments complex.

d. I later saw SCHEMER#9 walk towards building 10987 at the Avalon Apartments complex. Later that day while observing the pole camera directed at the balcony of SUBJECT PREMISES #1, I observed SCHEMER#9 with SCHEMER#8 on the balcony of SUBJECT PREMISES #1. I also observed SCHEMER#9 close the blinds to SUBJECT PREMISES #1.

e. By subsequently reviewing video surveillance, I later confirmed that SCHEMER#9 exited SUBJECT PREMISES #1 at approximately 3:07 p.m., with his jacket and documents in hand. He was also accompanied by UF1.

f. I researched the license plate of the vehicle driven by SCHEMER#9 on March 29, 2016, and found that the vehicle was registered to Rafik Martirosyan. I examined the California Driver's License photo of Rafik Martirosyan and found that that person does not resemble SCHEMER#9.

10. SCHEMER#10: Konstantin Galstyan

172. Based on the facts immediately following, I believe that Konstantin Galstyan (SCHEMER#10), posing and using fraudulent identification in different identities that were not his true identity, rented at least two mailboxes and opened at least 4 bank accounts that were used in this scheme. Below are the details of the mailboxes rented by SCHEMER#10 and the bank accounts opened by SCHEMER#10, and the identifications in different identities that he used to do so.

173. On October 24, 2013, box #105 at C & E Mailboxes, 5082 W. Pico Blvd., Los Angeles, California, was rented in the name

of "Robert Hovhannisyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AH0550821 and Costco membership card number 111829114576, both in the name of "Robert Hovhannisyan." Both of those identification documents appear to have the photograph of SCHEMER#10.

174. On June 17, 2014, box #203 at Mail Monster, 941 S. Vermont Ave., Ste. 101, Los Angeles, California, was rented in the name of "Levon Karapetyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AM0580770 in the name of "Levon Karapetyan" that had SCHEMER#10's photograph on it.

175. I have examined the Armenian passports in the name of Robert Hovhannisyan and Levon Karapetyan and the Costco membership card in the name of Robert Hovhannisyan, and I have compared them to the California driver's license issued to SCHEMER#10. Based on that comparison, I believe that all of the photo identifications are the same person, SCHEMER#10.

176. The Republic of Armenia informed the U.S. Embassy in Armenia that Republic of Armenia passport numbers AH0550821 and AM0580770 were issued in the names of Robert Hovhannisyan and Levon Karapetyan, respectively. Therefore, I believe that Republic of Armenia passport numbers AH0550821 and AM0580770 were altered to display SCHEMER#10's image, and then used to rent mailboxes as part of this scheme.

177. A review of Citibank account 203591979 in the name of Zig Zag Jewelry and Union Bank account 901102525 in the name of Garo Minassian shows that each bank account was used as a Tier-3 bank account in this scheme, and that each bank account had a deposit in 2014 consisting from "Levon Kerapetyan" (sic). Those checks were drawn on Bank of America account 325027344644 and had the address of 941 S. Vermont Ave., Ste. 101, Los Angeles, California. Although at this time I do not have the records for Bank of America account 325027344644, I believe that SCHEMER#10, posing in the identity of "Levon Kerapetyan," opened Bank of America account 325027344644.

178. I have reviewed JPMorgan Chase Bank records for bank account 566129859. That bank account was opened on February 18, 2014, in Los Angeles, California, in the name of Robert Hovhannisyan DBA H & R Jewelers, with address 5082 W. Pico Blvd., Apt. 105, Los Angeles, California. That bank account had two deposits in February 2014 from three checks drawn on Tier-1 bank accounts. I believe that SCHEMER#10, posing in the identity of "Robert Hovhannisyan," opened JPMorgan Chase Bank account 566129859.

a. In addition to the bank accounts described above, I have reviewed additional bank records that show there were at least three other bank accounts opened in the name in the name of "Robert Hovhannisyan."

179. According to JPMorgan Chase Bank records, account 231526506 was opened on July 8, 2013, in Los Angeles, California

in the name of "Abraham Hovhannisyan." The address on the signature card and statements is 404 W. 7th St., Ste. 1226, Los Angeles, California. Account 231526506 operated as a Tier-2 bank account in this scheme in 2013, with check deposits and outgoing payments to Newport Precious Metals. The bank records also include a photographic identification for "Abraham Hovhannisyan" in the form of an Armenian passport. I have compared that passport photograph to the California driver's license photograph of SCHEMER#10, and based on that comparison, I believe they are the same person, and that SCHEMER#10, posing in the identity of "Abraham Hovhannisyan," opened JPMorgan Chase Bank account 231526506 in the name of "Abraham Hovhannisyan."

180. According to JPMorgan Chase Bank records, account 171699320 was opened on January 28, 2013, in Los Angeles, California, in the name of Abraham Hovhannisyan DBA Abraisyan Jewelry. The address on the signature card and statements is 404 W. 7th St., Ste. 1226, Los Angeles, California. Account 171699320 operated as a Tier-2 bank account in this scheme during 2013, with check deposits and outgoing payments to Newport Precious Metals. The bank records also include a photographic identification for "Abraham Hovhannisyan" in the form of Armenian passport number AH0511336. I have compared the photograph on that passport to the California driver's license photograph of SCHEMER#10, and based on that comparison, and I believe they are the same person.

181. The Republic of Armenia informed the U.S. Embassy in Armenia that passport number AH0511336 was issued in the name of Abraham Hovhannisyan. Therefore, I believe that Republic of Armenia passport number AH0511336 was altered to display SCHEMER#10's image, and then used to open JPMorgan Chase Bank account 171699320 as part of this scheme.

182. I have examined a photograph of a male individual provided by JPMorgan Chase Bank who was photographed while depositing a \$1,920 check from "Aghavni Baghdasaryan" payable to Harhak Dimonds (sic) on February 25, 2014. The check was drawn on Citibank bank account 42011250430, a known Tier-2 bank account, and was deposited to JPMorgan Chase Bank account 559286559 in the name of Hakob Harutyunyan DBA Harhak Diamonds, which is another known Tier-2 bank account. I believe that the male individual in the photograph is SCHEMER#10, and thus, as part of this scheme, SCHEMER#10 is shown depositing a check drawn on a known Tier-2 bank account into another Tier-2 bank account.

11. SCHEMER#11: Mkhitar Mkrtchyan

183. Based on the facts immediately following, I believe that Mkhitar Mkrtchyan (SCHEMER#11), posing and using fraudulent identification in different identities that were not his true identity, rented at least two mailboxes and opened at least two bank accounts that were used in this scheme. Below are the details of the mailboxes rented, and bank accounts opened, by SCHEMER#11, and the identifications in different identities that

he used to do so.

184. On October 24, 2013, box #375 at Wilshire Mail Box, 5042 Wilshire Blvd., Los Angeles, California, was rented in the name of "Hakob Harutyunyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AG0655017 and Costco membership card number 111829114346, both in the name of "Hakob Harutyunyan." The passport appears to have the photograph of SCHEMER#11, but the copy of the photograph on the Costco card is too poor to make a determination.

185. On October 24, 2013, box #107 at 4U Mailboxes, 505 S. Vermont Ave., Ste. B, Los Angeles, California, was rented in the name of "Gevorg Martirosyan." When opening that mailbox, the individual posing in that identity provided as identification Republic of Armenia passport number AK0575016 in the name of "Gevorg Martirosyan" that had SCHEMER#11's photograph on it.

186. I have examined the Armenian passport photographs in the names of "Hakob Harutyunyan" and "Gevorg Martirosyan" that were used as identification when the two private mailboxes were rented. I believe that the individual in the Armenian passport photographs is the same person, wearing the same shirt; in fact, I further believe that it might actually be the same photograph on the two passports. I have also examined and compared the Costco membership card and the California driver's license photograph of SCHEMER#11 and compared them to the Republic of Armenia passport photographs in the names of Hakob Harutyunyan

and Gevorg Martirosyan, and based on that comparison, I believe that they are all photographs of SCHEMER#11.

187. The Republic of Armenia informed the U.S. Embassy in Armenia that passport AG0655017 and AK0575016 were issued in the names of Hakob Harutyunyan and Gevorg Martirosyan respectively. Therefore I believe that Republic of Armenia passport numbers AG0655017 and AK0575016 were altered to display SCHEMER#11's image, and then used to rent mailboxes as part of this scheme.

188. I have reviewed bank records for "Hakob Harutyunyan," and I believe that SCHEMER#11, posing in the identity of Hakob Harutyunyan, opened two bank accounts that operated as Tier-2 bank accounts in this scheme, as described here:

a. According to Citibank records, checking account 42011323310 was opened on February 3, 2014, in the name of "Hakob Harutyunyan." The address listed on the signature card for that bank account is 610 S. Broadway, Apt. # 205, Los Angeles, California, and the address on the statements is 5042 Wilshire Blvd., Apt. 375, Los Angeles, California. Checking account 42011323310 operated as a Tier-2 bank account in this scheme during 2014 and 2015, with deposits of checks drawn from Tier-1 and Tier-2 bank accounts, and checks made payable to Tier-3 bank accounts, including LA Hoops, Unika, M & M Jewelry, and HD Jewelry in 2014 and 2015.

b. According to JPMorgan Chase records, bank account 559286559 was opened on February 3, 2014, in the name of Hakob Harutyunyan DBA Harhak Diamonds. The address listed on the

signature card is 5042 Wilshire Blvd., Ste. 375, Los Angeles, California. Except for an opening \$100 deposit, the deposits to the account consisted of checks drawn from Tier-2 bank accounts in the names of "Lilit Avetyan" and "Aghavni Baghdasaryan." One of these checks was described in the section for the previous schemer as being deposited by SCHEMER#10 on February 25, 2014.

189. I have examined a photograph provided by JPMorgan Chase Bank of a male who was photographed while depositing a \$3,610 check from "Lilt Avetyan" payable to Harhak Diamonds on February 26, 2014. The check was drawn on Wells Fargo Bank account 2609118043, an identified Tier-2 bank account in this scheme, and was deposited to JPMorgan Chase Bank account 559286559 in the name of Hakob Harutyunyan DBA Harhak Diamonds. The male appears to be wearing the same shirt as in the individual in the Armenian passport photographs of "Hakob Harutyunyan" and "Gevorg Martirosyan." I believe that the male shown depositing that check drawn on a known Tier-2 bank account to another Tier-2 bank account was SCHEMER#11.

190. In addition to the bank accounts described above, I have reviewed other bank records that show there were at least five more bank accounts opened in the name of "Hakob Harutyunyan."

191. I have reviewed bank records for "Gevorg Martirosyan," and I believe that SCHEMER#11, posing in the identity of Gevorg Martirosyan, opened two bank accounts that operated as Tier-2 bank accounts in this scheme, as described here:

a. According to Bank of America records, checking account 325024700867 and savings account 325024706706 were opened on November 5, 2013, in Los Angeles, California, in the name of "Gevorg Martirosyan." The opening documents list a permanent address of "35 Saryan St. # 4, Yerevan, Armenia," and a current address of 610 S. Broadway, Ste. 205, Los Angeles, California. The opening documents also list a foreign passport number AK0575016 (the same number of the Republic of Armenia passport discussed above that was used to open the mailbox in the name of "Gevorg Martirosyan"). The statements were initially addressed to 404 W. 7th St., Ste. 1226, Los Angeles, California, which is the same address that was listed on JPMorgan Chase accounts 231526506 and 171699320 in the names of Abraham Hovhannisyan and Abraham Hovhannisyan DBA Abraisyan Jewelry, respectively. Beginning with the statement beginning November 19, 2013, the statements were addressed to 505 S. Vermont Ave., Ste. B107, Los Angeles, California.

b. Bank of America account 325024700867 operated as Tier-2 bank account in this scheme during 2014 and 2015, while account 325024706706 operated as Tier-2 bank account during 2015 only. Both accounts had deposits consisting of checks drawn from Tier-1 and Tier-2 bank accounts. The vast majority of the funds deposited into account 325024706706 were then transferred to account 325024700867. Checks drawn on account 325024700867 were made payable to Tier-3 bank accounts, including to Chic Accessories, Unika, Zig Zag Jewelry, and HD Jewelry, during

2014. In 2015, there was a wire transfer from account 325024700867 to Newport Precious Metals. Both accounts were closed on March 12, 2015.

192. As mentioned above, SCHEMER#11 is also the owner and president of Zig Zag Jewelry, which had numerous bank accounts that were discussed above.

12. Other conspirators/schemers

a. SCHEMER#12: Marat Nazaryan

193. Based on surveillance operations, bank surveillance video and photos, and bank employee interviews, as discussed below, I believe that Marat Nazaryan (SCHEMER#12) is a member of this scheme, and his role is as a runner.

194. Other agents and I have followed SCHEMER#12 from SUBJECT PREMISES #1 to several banks where he was observed depositing checks into known and suspected Tier-2 and Tier-3 bank accounts.

195. As discussed above in the section on Tier-3 bank accounts, SCHEMER#11 has opened several bank accounts in the name of his company, Zig Zag Jewelry, and has used his bank accounts to launder the tax fraud proceeds in the scheme. I have reviewed bank records for Wells Fargo Bank account number 3052160060, which was opened in by SCHEMER#11. The account was opened in the name of SCHEMER#11 DBA Zig Zag Jewelry. According to the signature card, SCHEMER#11 opened the account on June 23, 2014. I also requested bank surveillance photos for all account deposits. I have reviewed the account deposits and matched them

with the bank and ATM photos. Bank surveillance photos show that on September 8, 2015, SCHEMER#12 deposited a check from a Tier-2 bank account drawn from a Union Bank bank account held in the name of "Sergey Kosakyan." Bank records also reveal that SCHEMER#12 submitted a deposit slip which specifically detailed the name on the account, "Zig Zag Jw" (sic) and Zig Zag's account bank account number.

196. As also discussed above, under the section on SCHEMER#6, I have reviewed bank account records related to Citibank account number 42013322211 in the name of "Anahit Israyelyan," which was opened by SCHEMER#6. I was also provided with bank surveillance photographs of check deposits to that bank account. I matched the deposit slips along with the checks to the bank surveillance photographs to determine who was actually making the deposits. From that review, I discovered that on March 6, 2015, SCHEMER#12 deposited a check drawn from a Tier-1 bank account from Bank of America account number 325030841833, opened in the name of "Khachatur Nersisyan," into the bank account in the name of "Anahit Israyelyan." IA Gilmore confirmed that Bank of America account number 325030841833 was used to deposit tax refunds from at least six false tax returns during 2015.

197. The investigation shows that SCHEMER#12 has been an active member of this money laundering scheme since at least 2015. SA Ou, other agents, and I have observed SCHEMER#12 enter and exit SUBJECT PREMISES #1 carrying checks and other unknown

documents. During several surveillance operations conducted in 2015 and 2016, I have seen SCHEMER#12 interact with and engage in conversations with other fraudsters at or around the Avalon Apartments complex, including with SCHEMER#1, SCHEMER#8, SCHEMER#9, SCHEMER#13, SCHEMER#14, SCHEMER#15, AND SCHEMER#16. Based on my own observations of SCHEMER#12, I believe he is a trusted runner in this scheme who is given regular access to SUBJECT PREMISES #1 and who is tasked with depositing checks into Tier-2 and Tier-3 bank accounts in this scheme.

198. I also believe SCHEMER#12 attempts to avoid being detected by law enforcement when driving to SUBJECT PREMISES #1 or to banks. For example, other agents and I have observed SCHEMER#12 drive vehicles that are not registered to him. He has also been observed via bank surveillance photos, talking on his cell phone or acting as if he were talking to someone on his phone while making deposits into Tier-2 bank accounts in this scheme. I believe SCHEMER#12 engages in such behavior to make him appear less suspicious to the bank employees and to investigators.

b. SCHEMER#13: Arman Abrahamyan

199. As discussed in the section on the IRS-CI and FBI Seattle Investigation, Arman Abrahamyan (SCHEMER#13) and other targets described in this affidavit were identified as also being involved in that separate investigation. Based on this investigation, I believe the individuals and locations identified in the Seattle Investigation, including SCHEMER#1,

SCHEMER#13, SCHEMER#11, Zig Zag Jewelry, and SUBJECT PREMISES #2, continued to facilitate the fraud in this scheme.

200. I discovered SCHEMER#13's involvement in this scheme on August 11, 2015, when he was talking to SCHEMER#12 at the Avalon Apartments complex. During several surveillance operations, I have also seen SCHEMER#13 engage in conversations on the balcony of SUBJECT PREMISES #1 with suspected ring leader SCHEMER#1, runners such as SCHEMER#15, and Tier-2 bank account holders SCHEMER#8 and SCHEMER#9.

201. Based on this investigation, I believe SCHEMER#13 acts as a handler to some of the Tier-2 bank account holders and as someone who manages SUBJECT PREMISES #1 for the money laundering crew. Other agents and I have also observed SCHEMER#13 drive Tier-2 bank account holders to banks to engage in fraud as part of this schemer have observed SCHEMER#13 drive with Tier-2 bank account holders to private mailboxes to open new mailboxes or pick up mail there.

202. Like SCHEMER#12, I believe that SCHEMER#13 conducts counter-surveillance techniques to avoid being detected by law enforcement. For example, on September 22, 2015, HSI agents and I followed SCHEMER#13 from the Avalon Apartments complex. SCHEMER#13 was driving a vehicle that was not registered to him. During the mobile surveillance, agents observed SCHEMER#13 and an unknown passenger, pull off to the side of road on Vineland Ave. on top a bridge. The Los Angeles River runs under that bridge. The passenger was observed exiting the vehicle and

throwing several crumbled up documents into the river. Agents then observed SCHEMER#13 making an abrupt U-turn and looking around and through his rear view mirror. Based on my training and experience, I believe SCHEMER#13 was conducting counter surveillance.

c. SCHEMER#14: Harutyun Sukiasyan.

203. During surveillance operations in 2015 and 2016, I have observed Harutyun Sukiasyan (SCHEMER#14) visit known locations, including SUBJECT PREMISES #1, where SCHEMER#1, the suspected ring leader of this money laundering scheme, and other runners visit to discuss and carry out this money laundering scheme.

204. On multiple surveillances, SA Ou and I have observed SCHEMER#14 with SCHEMER#16, also a known runner in this scheme, as discussed below. Both have also been seen together at Chic Accessories, as well as at SUBJECT PREMISES #1.

205. On August 19, 2015, I observed SCHEMER#14 drive and park on Vineland Ave. in Studio City, California. SCHEMER#14 was driving a grey Mercedes Benz with license plate number 7JWP065. I ran the license plate number in the California Department of Motor Vehicle database and found that the vehicle was actually registered to SCHEMER#3. As previously discussed, using other individuals' identities, SCHEMER#3 opened at least two Tier-2 bank accounts in this scheme. SCHEMER#14 exited SCHEMER#3's vehicle and walked into the Avalon Apartments complex.

206. I have taken multiple photographs of SCHEMER#14 while he stood on the balcony of SUBJECT PREMISES #1 talking to SCHEMER#1 and other known runners and Tier-2 bank account holders of this scheme.

207. I obtained SCHEMER#14's criminal history report and found that he has several arrests dating back to 2005. His rap sheet includes violations of possession of bad checks, receiving stolen property, burglary, grand theft, DUI causing bodily injury, driving on a suspended license, forged prescriptions, credit fraud with respects to identity theft, infliction of corporal injury to his spouse, vandalism, and hit and run. In 2012, SCHEMER#14 was convicted for felony possession of a firearm and using account information without consent, and was sentenced to two years in prison.

d. SCHEMER#15: Albert Andriasov

208. Albert Andriasov (SCHEMER#15) is another runner in this scheme. Bank surveillance photos taken in 2015 and recent surveillance of SCHEMER#15 confirm that he has transacted on known Tier-2 bank accounts and has driven multiple Tier-2 bank account holders, including SCHEMER#6 and SCHEMER#8, to banks in an attempt to obtain funds from Tier-2 bank accounts used in this scheme.

209. SCHEMER#15's criminal history report shows that his driver license has been suspended since April 3, 2013.

210. Since March 2015, I have seen SCHEMER#15 drive at least two vehicles on a regular basis. The VIN and license

plate were researched and found to have been registered to two different individuals. SA Ou and I have seen SCHEMER#15 drive these vehicles to and from Chic Accessories and SUBJECT PREMISES #1 during several surveillance operations.

211. Most recently, on January 22, 2016, SCHEMER#15 was escorting SCHEMER#6 to a Citibank branch in Los Angeles, California. Multiple Citibank employees observed SCHEMER#15 driving in a black Range Rover with dealer plates. I observed SCHEMER#15 later that day arriving at the Avalon Apartments complex in the same vehicle. This vehicle is registered to Ashot Hakhverdyan.

212. In March 2016, I was notified by Citibank of an account takeover involving one of their customers. Beginning on December 28, 2015, through January 28, 2016, 13 counterfeit checks were drawn from a Citibank bank account and deposited into two Tier-2 bank accounts held at Bank of America that were also used in this scheme. The loss to the bank from that account takeover was approximately \$64,000.

213. On March 29, 2016, Bank of America provided me with bank surveillance photos of a person depositing the counterfeit Citibank checks into known Tier-2 bank accounts, on December 31, 2015, and on January 27, 2016. I reviewed the photos and recognized the person in the bank surveillance photos to be SCHEMER#15.

214. I believe SCHEMER#15 and the other fraudsters who frequent SUBJECT PREMISES #1 are also involved in account

takeover schemes and use SUBJECT PREMISES #1 to safe keep checks related to those other schemes they are also orchestrating. For example, on January 27, 2016, I observed SCHEMER#1, SCHEMER#8, SCHEMER#9, and SCHEMER#15 on the balcony of SUBJECT PREMISES #1. I followed SCHEMER#8 and SCHEMER#9 from SUBJECT PREMISES #1 to Bank of America and several private mailboxes, where I confirmed that SCHEMER#9 had opened a bank account and SCHEMER#8 had opened a private mailbox, both using passports from the country of Georgia. In addition, as discussed in the previous paragraph, on January 27, 2016, at approximately 1:55 p.m., Bank of America bank surveillance captured SCHEMER#15 depositing a counterfeit Citibank check. That check was deposited into a Tier-2 bank account opened in the name of "Robert Havel." According to my surveillance report for January 27, 2016, I observed SCHEMER#15 and SCHEMER#9 exit SUBJECT PREMISES #1 at approximately 1:41 p.m. and drive away from the Avalon Apartments complex in SCHEMER#15's black Range Rover. Thus, I believe SCHEMER#15 drove directly from SUBJECT PREMISES #1 to the bank to deposit that counterfeit check. I further believe he was probably provided this check at SUBJECT PREMISES #1.

215. This is the second account takeover scheme that I have been made aware since October 2015. In each case, known Tier-2 bank accounts were used to funnel stolen money from Wells Fargo and Citibank customers. I have reviewed Citibank ATM photographs and Bank of America branch surveillance photographs

and have identified runners like SCHEMER#12 and SCHEMER#15 also making deposits into Tier-2 bank accounts in this scheme.

e. SCHEMER#16: Tigran Galstyan

216. As discussed below, Tigran Galstyan (SCHEMER#16) appears to be involved in the scheme in the capacity of driving known schemers to and from SUBJECT PREMISES #1 and Chic Accessories.

217. In or around September 2014, HSI SA Ou and I met with FBI SAs and presented several passport photographs that were used in this scheme to open Tier-2 bank accounts using other individuals' identities, specifically passports in the names of "Artur Virabyan," "Hamlet Petrosyan," and "Hyak Yegorian." FBI agents researched that information using law enforcement databases and their own case files and confirmed that the person from those three passport photographs was actually the same person: SCHEMER#7.

218. FBI SA Matsumura told me that he and other agents of the FBI were investigating a Medicare/identity theft scheme in 2012 and 2013. Their investigation identified SCHEMER#7 and SCHEMER#16 as subjects of their investigation.

219. FBI SA Matsumura told me that in January 2013, SCHEMER#7 and SCHEMER#16 drove to San Luis Obispo to pick up a check that constituted proceeds of that scheme.

220. On or about February 18, 2015, HSI SA Ou and I conducted a knock-and-talk at SCHEMER#16's residence in Burbank, California. During the interview, we showed a photograph of

SCHEMER#7 to SCHEMER#16. Upon seeing that photograph, SCHEMER#16 became noticeably uncomfortable and suddenly told us that he was not feeling well. However, SCHEMER#16 did admit that he had been traffic stopped while driving SCHEMER#7, but SCHEMER#16 stated that SCHEMER#7 had simply asked him for a ride to San Luis Obispo. SCHEMER#16 said that he did not know the purpose of that trip.

221. On or about April 28, 2015, other law enforcement officers and I conducted a mobile surveillance of SCHEMER#16. I observed SCHEMER#16 enter Chic Accessories not carrying anything, remain inside for approximately 30 minutes, and then exit Chic Accessories carrying a black shoulder laptop bag that he had not had with him when he had entered Chic Accessories. We observed SCHEMER#16 place the black shoulder laptop bag into his vehicle and drive away. A mobile surveillance ensued. During that surveillance, SCHEMER#16 appeared to utilize counter-surveillance techniques.

222. In addition to the April 28, 2015, date when SCHEMER#16 was observed carrying out a black shoulder laptop bag from Chic Accessories, IRS-CI SA Ou and I have observed SCHEMER#16 come and go from Chic Accessories three other times: on April 1, 2015, April 22, 2015, and April 27, 2015.

223. Based on the above, I believe that SCHEMER#16 is also involved with this laundering scheme and is a runner for the laundering scheme.

224. On July 21, 2015, the Honorable Douglas F. McCormick authorized a tracker warrant on SCHEMER#16's vehicle.

225. On August 21, 2015, HSI SA Ou and I conducted a mobile surveillance of SCHEMER#16 in his vehicle. Agents observed SCHEMER#16 drive south on Verdugo Blvd. in Glendale and, until he drove into a residential street, make a U-turn and head north on Verdugo Blvd. in what appeared to be a counter-surveillance technique. SCHEMER#16 pulled over on Verdugo Blvd. approximately 3-5 blocks south of Colorado Blvd. SA Ou observed SCHEMER#16 exit his vehicle, flag someone down, and run across the street. I then observed SCHEMER#16 talking to Karen Karapetyan next to Karapetyan's bronze Lexus, which was parked on street. I observed Karapetyan showing SCHEMER#16 what appeared to be the contents of what was inside a white envelope. Previously, on August 11, 2015, and August 13, 2015, SA Ou and I saw Karapetyan at the Avalon Apartment complex interacting with SCHEMER#12 and SCHEMER#13.

f. SCHEMER#17: Haroutioun Demirdjian

226. As discussed above, Haroutioun Demirdjian (SCHEMER#17) is the current account holder of multiple Tier-3 bank accounts in this scheme. However, review of bank surveillance photographs and bank records from J.P. Morgan Chase Bank, Citibank, U.S. Bank, and Bank of America in 2014 and 2015 confirmed that SCHEMER#17 has also functioned as a "runner" for this laundering scheme. That is, SCHEMER#17 deposited checks

drawn from Tier-1 bank accounts into Tier-2 bank accounts at bank branches located throughout Southern California.

227. Bank surveillance photographs from the Seattle Investigation also suggest that SCHEMER#17 was involved in that scheme since at least 2012.

228. Since February 11, 2014, I have examined bank surveillance photographs of SCHEMER#17, while he was conducting transactions on known Tier-2 bank accounts, on approximately 20 occasions.

229. On or about March 19, 2015, March 26, 2015, April 1, 2015, April 22, 2015, and April 27, 2015, HSI SA Ou and I, and other members of law enforcement, conducted surveillance of SCHEMER#17 and Chic Accessories.

a. On each of those dates, we observed SCHEMER#17 visit Chic Accessories, and on three of those days, SCHEMER#17 was followed to banks where he then proceeded to deposit checks drawn on Tier-1 bank accounts into Tier-2 bank accounts.

b. On March 26, 2015, SCHEMER#17 was also followed to a post office box facility. HSI SA Ou and I spoke to an employee of that facility, who confirmed that SCHEMER#17 had picked up mail from two boxes there: 113 and 97. I confirmed that those two box addresses correspond to addresses that had been used to open Tier-2 bank accounts in this scheme.

I. During 2015, Chic Accessories, a Business in Hollywood, California, Was The Meeting and Storage Location From Which Various Schemers Originated Before Depositing Tier-1 Checks into Tier-2 Bank Accounts As Part of This Scheme.

230. As discussed above, SCHEMER#17 has been observed coming and going on multiple different dates from Chic Accessories, after which he went to banks to deposit checks drawn on Tier-1 bank accounts into Tier-2 bank accounts, or went to a post office box facility tied to the scheme.

231. On May 8, 2015, HSI SA Ou and I interviewed Rose Farkas and Ivi Winterman, owners of the building where Chic Accessories and the offices on the second floor are located. Farkas and Winterman stated the following:

a. Farkas and Winterman lease 6519 Hollywood Blvd., Hollywood, California, to business Chic Accessories.

b. The business named Chic Accessories is owned by Suzy Seraydarian.

c. Moses Seraydarian is Suzy Seraydarian's wife.

d. Moses Seraydarian also rents office space #214 from Farkas. He was on a month-to-month lease.

e. Moses Seraydarian told her that he used the office space to store shoes and other items related to Chic Accessories.

f. A digital code and key is needed to gain access to the second floor offices. Farkas gave Moses Seraydarian both a key and the code combination.

g. Moses Seraydarian has access only to office #214. He has rented this office for a few years.

h. Office #214 is approximately 400 square feet.

232. The address listed for the offices is 6513 Hollywood Blvd., Los Angeles, California. A small door, located on Hollywood Blvd., leads to the second floor offices. The access point to the offices on the second floor is a door located next door to Chic Accessories.

233. On March 26, 2015, SAs observed SCHEMER#17 leaving Chic Accessories and driving directly to various banks to deposit several checks linked to bank accounts that had been used to receive fraudulent tax refunds. SCHEMER#17 was observed returning to Chic Accessories to pick up Moses Seraydarian.

234. On April 1, 2015, IRS and HSI SAs conducted a surveillance operation outside of Chic Accessories. A digital camcorder was used to record the activity of the known runners in the scheme and their activity in and around Chic Accessories. During the surveillance operation, the following events were observed in connection with Chic Accessories and office #214:

a. At approximately 10:00 a.m., Moses Seraydarian arrived and opened Chic Accessories to the public.

b. Moses Seraydarian was observed walking in and out of Chic Accessories and having conversations with an unknown male, subsequently identified as SCHEMER#15. SCHEMER#15 is described as an Armenian male, approximately 25-30 years of age, medium size, having a dark beard, and dark hair.

c. At approximately 12:00 p.m., SCHEMER#16 was observed entering Chic Accessories. Then, at approximately 12:20 p.m., SCHEMER#17 entered Chic Accessories. Then, at approximately 12:23 p.m., SCHEMER#16 exited Chic Accessories, and returned at approximately 12:48 p.m. Then, at approximately 12:53 p.m., SCHEMER#17 exited Chic Accessories, went to his vehicle, retrieved something from his vehicle, returned to Chic Accessories, and re-entered. At approximately 1:04 p.m., SCHEMER#17 exited Chic Accessories, went to his vehicle, retrieved something from his vehicle, returned to Chic Accessories, and re-entered.

d. Surveillance was not able to view SCHEMER#16 and SCHEMER#17 leaving Chic Accessories, but at 2:14 p.m., SCHEMER#16 returned to Chic Accessories, and SCHEMER#14 removed a crate from SCHEMER#16's vehicle and brought the crate to the doorstep of Chic Accessories while SCHEMER#16 parked his vehicle. Then, SCHEMER#16 entered Chic Accessories, remained for several minutes, and then with help from several other men, carried the crate into the second-story office located adjacent to Chic Accessories.

235. On April 22, 2015, at approximately 1:35 p.m., HSI SA Ou and I observed SCHEMER#17 walk into Chic Accessories empty handed. Approximately five minutes later, SCHEMER#16 and two unknown Armenian males walked into Chic Accessories.

a. Shortly after entering Chic Accessories, SCHEMER#16 and the other men walked through the door that leads up to office #214.

b. SCHEMER#17 then exited Chic Accessories at approximately 1:50 p.m. holding in his hands what appeared to be white envelopes, and he walked directly to his vehicle and drove off.

236. On April 27, 2015, a surveillance operation was conducted outside of Chic Accessories and of SCHEMER#17's residence.

a. SCHEMER#17 was followed from his residence to Chic Accessories.

b. SCHEMER#17 was then subsequently exiting Chic Accessories carrying what appeared to be envelopes. SCHEMER#17 then drove directly to JPMorgan Chase bank located at 1500 Vine, Los Angeles, California, and the Comerica Bank located at 6255 Sunset Blvd. #100, Los Angeles, California 90028. I confirmed with Chase and Comerica fraud investigators that SCHEMER#17 had deposited checks drawn from Tier-1 bank accounts into Tier-2 bank accounts, including into his own business bank account held in the name of H.D. Jewelry Inc. at Comerica Bank.

c. At approximately 4:32 p.m., HSI SA Ou and I observed a male adult enter and walk through the door that leads to office #214 carrying what appeared to be a large FedEx envelope. That individual appears to be the same person who had been seen on April 1, 2014, talking to Moses Seraydarian outside

of Chic Accessories. HSI SA Ou told me that he believed that individual was SCHEMER#15.

237. U.S. Bank provided me with surveillance photographs of deposits made into the bank account in the name of "Artur Pogohsyan" on March 19, 2015. Based on my review of those U.S. Bank surveillance photographs, the individual carrying the FedEx envelope matches the description of and looks like the person making the deposit at the U.S. Bank located at 9476 West Third St., Los Angeles, California, at approximately 10:47 a.m.

238. After reviewing bank account records for Tier-1 and Tier-2 bank accounts used in this scheme, I know that these bank accounts were opened with commercial mailboxes used as the account holder's residence. As described above, these commercial mailboxes and bank accounts were often opened using fraudulent Armenian passports where the photo displayed on the passports is on other Armenian passports to open additional bank accounts used in this scheme. The control over these mailboxes is a critical part in operating this scheme. The perpetrators primarily use the mailboxes for the purpose of receiving checkbooks from the financial institutions where Tier-1 and Tier-2 bank accounts are opened and correspondence from banks like cashier checks. Based on my conversations with Citibank and Bank of America fraud investigators, I know that Citibank and Bank of America will send cashier checks for the amount of the remaining bank account balance to the address on file, after the account has been closed by the bank.

239. On April 28, 2015, IRS-CI and HSI SAs conducted a surveillance operation outside of Chic Accessories.

a. During the operation, SCHEMER#16 and SCHEMER#17 were observed walking into Chic Accessories.

b. At approximately 3:17 p.m., SCHEMER#16 exited Chic Accessories carrying a laptop computer bag. He placed the computer bag into his vehicle and drove away.

c. SAs followed SCHEMER#16 as he drove to the city of Glendale via side streets. While following SCHEMER#16, agents noticed that he was conducting counter surveillance techniques. Due to this reason, the agents discontinued surveillance of SCHEMER#16.

240. Thus, I believe that Chic Accessories was the source of the checks from Tier-1 bank accounts that were being deposited into Tier-2 bank accounts during 2015.

241. I spoke to the owner of the building who was renting to Chic Accessories, who told me that the Seraydarians stopped renting Unit #214 in approximately June 2015. As noted in the following section, the schemers began to rent SUBJECT PREMISES #1 in June 2015.

J. There is Probable Cause to Believe That Evidence of This Scheme Will be Found at SUBJECT PREMISES #1, Which Is An Apartment Used as a Hub of Operations and Meeting Place for the Schemers.

1. Introduction and Summary

242. SUBJECT PREMISES #1 is a one bedroom apartment, Number

4209, located on the second floor of building number 10987 in the Avalon Apartments complex, which is located in Studio City, California.

243. On August 3, 2015, agents followed SCHEMER#16, who was discussed above as a known associate of this money laundering ring, to the Avalon Apartments complex.

244. After multiple surveillance operations, as discussed in depth below, we discovered that the schemers were using SUBJECT PREMISES #1 as a meeting place and hub of operations for this scheme. Specifically, as described immediately following, we were able to observe known schemers entering and exiting SUBJECT PREMISES #1:

a. On August 7, 2015, I observed SCHEMER#12 and SCHEMER#16 exit the Avalon Apartment complex together.

b. On August 11, 2015, I observed SCHEMER#12 enter SUBJECT PREMISES #1. Prior to my observing SCHEMER#12 entering SUBJECT PREMISES #1, HSI SA Ou had followed SCHEMER#12 to a Wells Fargo bank and observed him deposit a check into a bank account. (SA Ou and I later discovered that that bank account on which SCHEMER#12 had transacted was in fact a Tier-2 bank account used in this scheme.)

c. That same day, the Avalon Apartment manager provided me with leasing records for SUBJECT PREMISES #1. I reviewed those records and found that SUBJECT PREMISES #1 was rented in the name of "Tsalok Sozamyman" beginning on June 1, 2015. According to the leasing records, "Tsalok Sozamyman"

151

indicated that he was currently residing at 5632 Van Nuys Blvd., Van Nuys, California. This location is actually a CMRA and not a residence. In fact, at least four private mail boxes were opened at that location by schemers unknown to the investigation. These mailboxes were eventually used to open Tier-2 bank accounts in this scheme.

d. On April 12, 2016, I spoke with an Avalon Apartment leasing officer who informed me that "Tsalok Sozamyman" would not be renewing his lease, and his move out date will be May 31, 2016. "Tsalok Sozamyman" also informed the Avalon Apartments that he would be moving and provided address 5632 Van Nuys Blvd., Apt. 8, Van Nuys California, as his forwarding address. However, as mentioned in the above paragraph, that address is a CMRA and not an apartment building or a residential location. In fact, I have reviewed records for mail box #8, at 5632 Van Nuys Blvd., Van Nuys, California, and discovered that the mail box is rented in the name of "Tsolak Sazhumyan." I have reviewed the rental application for mail box #8 and the Republic of Armenia passport in the name of "Tsolak Sazhumyan" that was provided to the CMRA, and I discovered that the photograph displayed on the passport is someone whom I recognized in other passports in different names that were used in the scheme to open mailboxes. The person in the passport appears to be 50-60 years old and heavyset, whereas the individual who posed as "Tsalok Sozamyman" to rent SUBJECT

PREMISES #1 at the Avalon Apartments complex is described to be in his 20s.

245. Based on my review of the records used to rent SUBJECT PREMISES #1, my interview with Avalon Apartments leasing officers and manager, and the observations made during surveillance operations of SUBJECT PREMISES #1, I believe the fraudsters leased the apartment using a false identity.

a. Based on my training and experience, identity theft schemers often rent locations using false identities for the purpose of running their day-to-day illegal money laundering operations, which I believe is why the schemers rented SUBJECT PREMISES #1, and moreover, why they rented it in a false identity.

b. Based on my experience in identity theft investigations and conversations with other law enforcement officers and agents regarding organized crime, I know that criminals also lease cars and apartments using stolen identities in order to disguise, hide, or conceal their location from law enforcement so that they can continue operating their illegal activity.

c. The information provided to rent SUBJECT PREMISES #1 is false:

i. According to the lease file for SUBJECT PREMISES #1, an individual posing as "Tsalok Sozamyam" presented a California driver's license number E3146542 when renting SUBJECT PREMISES #1. I ran that driver license number in the

California Department of Motor Vehicles (DMV) data base and found no matching record.

ii. On the documents received from the Avalon Apartments complex that I reviewed, "Tsalok Sozamyman" indicated that he works for Warner Brothers Entertainment in Burbank, California, as an "International Billboard Manager" who earns an annual salary of \$105,000. To verify that information, I issued a subpoena to Warner Brothers Entertainment, and on or about November 9, 2015, Warner Brothers Entertainment responded that they had no records of "Tsalok Sozamyman" working for Warner Brothers Entertainment.

d. Based on my and other agents' observations of that apartment, I believe that SUBJECT PREMSIES #1 is vacant generally after 7:00 p.m., and in fact, no one actually lives there.

e. In addition, on or about August 11, 2015, I interviewed Monica Tockman, who identified herself as the leasing officer who had actually moved in "Tsalok Sozamyman" into SUBJECT PREMISES #1. Based on my interview with Tockman, I know that three men had originally wanted to rent an apartment for "Tsalok Sozamyman," who was not present at the time. The three men refused a tour of the apartment complex and were eager to rent any available apartment. The following day, one of the three men returned with someone who identified himself as "Tsalok Sozamyman." According to Tockman, the man helped "Tsalok Sozamyman" complete the leasing application. Tockman told me

that she has not seen "Tsalok Sozamyant" since she gave him the key to SUBJECT PREMISES #1 in June 2015. Furthermore, on March 3, 2016, Tockman told me that "Tsalok Sozamyant" had walked into the leasing office and inquired where to mail his rent checks. "Tsalok Sozamyant" told Tockman that he has been away and his friends have been making the rent payments for him. Tockman recognized the person who she spoke with as the same person who she moved into SUBJECT PREMISES #1 in June 2015.

246. Once we had identified SUBJECT PREMISES #1 as a location used in the scheme, as described below, we began extensive surveillance of SUBJECT PREMISES #1, which included using a pole camera, using the apartment directly underneath SUBJECT PREMISES #1, and direct observations from multiple locations in the Avalon Apartments complex, to identify individuals involved in this scheme.

247. On or about September 2015, we set up a pole camera that was facing the balcony of SUBJECT PREMISES #1, which operated from September 4, 2015, to November 3, 2015, and from January 12, 2016, to present.

248. Since August 3, 2015, I have conducted over forty surveillance operations of SUBJECT PREMISES #1 by using surveillance cameras, such as a pole camera, and GPS trackers on the vehicles driven by known runners. On several dates, I have seen known and unknown individuals tied to the scheme enter and exit SUBJECT PREMISES #1 carrying documents and other items such as bags, where the schemers were then followed to banks where

they produced and used checks and fictitious passports. In addition, I have observed suspected ring leader SCHEMER#1 carry a dark colored satchel or laptop carrier (SUBJECT BAG #1) in and out of SUBJECT PREMISES #1 at least 11 times.

249. Through this years-long investigation, as discussed below, we have also identified the following known associates to frequent SUBJECT PREMISES #1 on a regular basis: SCHEMER#1 (Gagik Airapetian), SCHEMER#5 (Hripsime Avagyan), SCHEMER#8 (Eduard Astvatsatryan), SCHEMER#9 (John Doe), SCHEMER#12 (Marat Nazaryan), SCHEMER#13 (Arman Abrahamyan), SCHEMER#14 (Harutyun Sukiasyan), SCHEMER#15 (Albert Andriasov), SCHEMER#16 (Tigran Galstyan), and Unidentified Female 1 ("UF1"), and other as-yet unidentified individuals. The following chart depicts dates when these schemers were observed in and or around SUBJECT PREMISES #1:

DATE	SCHEMER#1	SCHEMER#5	SCHEMER#8	SCHEMER#9	SCHEMER#12	SCHEMER#13	SCHEMER#14	SCHEMER#15	SCHEMER#16	UF1
8/3/15		x							x	
8/7/15		x			x					
8/11/15					x				x	
8/13/15		x			x					
8/19/15					x				x	
9/17/15	X								x	
9/21/15	X									
9/24/15		x							x	
9/28/15	X								x	

DATE	SCHMIDT 1/1	SCHMIDT 1/2	SCHMIDT 1/3	SCHMIDT 1/4	SCHMIDT 1/5	SCHMIDT 1/6	SCHMIDT 1/7	SCHMIDT 1/8	SCHMIDT 1/9	SCHMIDT 1/10	SCHMIDT 1/11
9/29/15		X			X				X		X
10/9/15		X							X		
11/13/15	X										
12/1/15	X		X		X			X	X	X	
12/3/15			X		X						X
12/7/15			X							X	X
12/9/15			X								
12/23/15									X		X
1/4/16			X							X	
1/5/16			X								
1/7/16						X	X	X		X	
1/12/16	X							X	X	X	X
1/13/16					X			X	X	X	
1/14/16			X	X	X					X	
1/20/16		X								X	
1/22/16	X		X	X				X		X	X
1/27/16	X		X	X				X		X	X
2/3/16	X		X	X							
2/4/16	X		X	X						X	
2/8/16			X	X		X				X	
2/9/16	X	X							X	X	
2/10/16	X	X		X				X		X	X
2/11/16	X	X	X	X	X			X	X	X	X
2/12/16	X	X	X	X				X		X	X
2/23/16	X		X	X				X		X	X

	SCHEMER #1	SCHEMER #2	SCHEMER #3	SCHEMER #4	SCHEMER #5	SCHEMER #6	SCHEMER #7	SCHEMER #8	SCHEMER #9	SCHEMER #10	SCHEMER #11	SCHEMER #12	SCHEMER #13
2/24/16	X		x	x	x	x			x	x		x	
2/25/16	x			x					x	x			
2/26/16	x			x					x			x	
2/29/16									x	x			
3/3/16	x							x	x	x			

2. Tier-2 bank account holders use SUBJECT PREMISES #1 as part of this scheme.

250. The following surveillance operations highlight dates and times that runners and other known schemers have been observed transporting documents, or traveling, to and from SUBJECT PREMISES #1.

251. August 11, 2015:

a. On August 11, 2015, at approximately 11:45 a.m., HSI SA Ou observed SCHEMER#13 exit the apartment complex next to the Avalon Apartments and meet with SCHEMER#12. SA Ou and I recognized SCHEMER#12 because he had been identified to us by Citibank bank personnel as an individual depositing checks tied to the scheme; we had also seen him on video stills provided by Citibank that showed him at the bank depositing checks into Tier-2 bank accounts. SA Ou followed SCHEMER#12 from SUBJECT PREMISES #1 to the Wells Fargo Bank in Studio City, California. SA Ou followed SCHEMER#12 into the bank and observed him deposit a check. SA Ou told me that he overheard SCHEMER#12 tell the

bank teller that the account or check was not his and that it was for someone else.

i. On a later date, SA Ou was later informed by Wells Fargo Fraud Investigator that the check was deposited by SCHEMER#12 into an account in the name of "Gagik Yeghiazaryan." I subsequently subpoenaed Wells Fargo Bank for the records for that bank account and once received, reviewed the corresponding bank statements and deposits. By that review, I confirmed that that bank account was being used as a Tier-2 bank account in this scheme.

ii. I also subpoenaed Bank of America for records related to accounts opened in the name of "Gagik Yeghiazaryan." Bank of America responded with records for two additional bank accounts. I reviewed these records and learned that in June 2014, two Bank of America bank accounts had been opened in that name. The accounts appeared to be inactive until three tax refunds totaling \$22,627 were deposited into one of the accounts in April 2015. IRS Investigative Analyst Gilmore confirmed that those three tax refunds had been generated by false tax returns.

b. At approximately 2:30 p.m., SA Ou observed SCHEMER#12 return to the Avalon Apartments complex and park his vehicle on Bluffside Drive. During this time I was standing in front of the apartment next to SUBJECT PREMISES #1. I was notified by SA Ou that SCHEMER#12 was walking into the Avalon

Apartments. At approximately 2:40 p.m., I observed SCHEMER#12 knock on the door and enter SUBJECT PREMISES #1.

252. August 13, 2015: On August 13, 2015, at approximately 1:47 p.m., SA Ou and I observed SCHEMER#12's vehicle parked across the street from the Avalon Apartments complex. At approximately 2:24 p.m., I saw SCHEMER#12 walk out of the Avalon Apartments complex holding a red bag. He entered his vehicle and drove away.

253. August 19, 2015: On August 19, 2015, at approximately 2:25 p.m., SA Ou and I observed SCHEMER#12 walk out of the Avalon Apartments complex carrying a white envelope. We followed him to two J.P. Morgan Chase Bank locations, one Bank of America location, and one Union Bank location. Fraud investigators from those banks provided me with photos taken from inside the banks, which I reviewed. SCHEMER#12 was captured by bank surveillance cameras walking into the Bank of America and Union Bank branches carrying a white envelope and depositing third party checks into accounts where he did not have signature authority. At approximately 3:16 p.m., SCHEMER#12 returned to the Avalon Apartments complex.

254. September 21, 2015: On September 21, 2015, I was monitoring the pole camera live, observing SUBJECT PREMISES #1. The pole camera faces the balcony of SUBJECT PREMISES #1. At approximately 5:25 p.m., I observed SCHEMER#1 talking on his cell phone at SUBJECT PREMISES #1. Approximately five minutes later, I observed SCHEMER#14 standing on the balcony of SUBJECT

PREMISES #1 holding an 8x11 manila envelope, and SCHEMER#14 appeared to be showing an unknown male the contents of the envelope.

255. October 9, 2015: On October 9, 2015, at approximately 2:29 p.m., I saw SCHEMER#12 and an unknown male walk out of the Avalon Apartments complex. The unknown male was holding a white envelope. Both SCHEMER#12 and the unknown male entered the Mercedes Benz registered to SCHEMER#3, a known Tier-2 bank account holder, and drove away.

256. December 1, 2015:

a. On December 1, 2015, I was notified by a Citibank fraud investigator that on November 30, 2015, Citibank account holder "Hrant Abovyan" had walked into the Citibank Branch located at 1900 W. Sunset Blvd., Los Angeles, California, and demanded that his bank accounts remain open and his funds be available for withdrawal. The individual who was posing as "Hrant Abovyan" told the bank he planned on coming back into the branch the following day, which was December 1, 2015. After receiving this information, HSI SA Ou, IRS-CI SA Leonard, and I conducted a surveillance operation outside of the bank in anticipation that the individual posing as "Hrant Abovyan" would return as promised.

b. At the time of the surveillance operation, we had not yet identified the true identity of the person who had opened the account under the name "Hrant Abovyan" and was posing as "Hrant Abovyan." However, we later identified the individual

posing as "Hrant Abovyan"'s to be SCHEMER#8. As previously discussed, SCHEMER#8 opened multiple Tier-2 bank accounts in this scheme from 2014-2016 using different identities and foreign passports, including the Citibank account under the name "Hrant Abovyan."

c. At approximately 12:05 p.m., I watched SCHEMER#8 walk into the Citibank Branch. Then, I received a text message from Rita Yolian, Citibank Branch Manager, that "Hrant Abovyan" had entered the bank. Yolian told me that SCHEMER#8 identified himself as "Hrant Abovyan" and provided a Republic of Armenia passport bearing the name "Hrant Abovyan" and SCHEMER#8's photograph. Yolian photocopied the passport and sent it to me via text. I recognized the person in the passport photograph to be SCHEMER#8. Yolian explained to SCHEMER#8 that Citibank had frozen "Hrant Abovyan"'s bank accounts because the bank suspected the bank account as being fraudulent because checks were deposited from bank accounts that had received several fraudulent tax refunds. Yolian told me that SCHEMER#8 claimed he was not aware of any tax refunds. Yolian told SCHEMER#8 that Citibank would be calling him after a review is performed on his bank account. At approximately 12:30 p.m., I observed SCHEMER#8 exit the bank and enter a white 2015 Lexus ES 350 bearing California license plate 7NSB040. SA Ou recognized the driver of the Lexus as SCHEMER#12, whom we had previously identified as a known runner of this scheme.

d. SA Ou, SA Leonard, and I followed SCHEMER#8 and SCHEMER#12 from Citibank to the Avalon Apartments complex.

e. At approximately 12:50 p.m., I observed SCHEMER#1, SCHEMER#8, SCHEMER#12, and UF1, all standing on the balcony of SUBJECT PREMISES #1.

f. From approximately 2:50 p.m. to 3:30 p.m., SA Ou and Los Angeles Police Detective A. Mkrtchyan positioned themselves in apartment 4109 of the Avalon Apartments complex, which is a permanently vacant apartment used as a display for future tenants. (Apartment 4109 is located directly underneath SUBJECT PREMISES #1 (which is Apartment 4209)). Permission to be inside apartment 4109 was granted by Avalon Apartment, and SA Ou was temporary provided the key to apartment 4109. While SA Ou and Detective Mkrtchyan were standing on the balcony of apartment 4109, I continued to monitor the balcony activity of SUBJECT PREMISES #1 through my binoculars. At approximately 3:25 p.m., I saw SCHEMER#13 walk out to the balcony and then re-enter the apartment. At the same time, SCHEMER#1 walked out onto the balcony of SUBJECT PREMISES #1 and began to talk on his cell phone. I immediately notified SA Ou that SCHEMER#1 was standing on the balcony. Detective Mkrtchyan, who speaks Armenian fluently, heard SCHEMER#1 say words in Armenian roughly translated as "we can't get it out." Based on the description above about what had occurred at the bank earlier that afternoon, i.e., that the bank employee had notified SCHEMER#8 that the bank had frozen the "Hrant Abovyan" bank accounts

because the bank suspected the account as being fraudulent, it appeared to me that SCHEMER#1 was talking to someone about that frozen bank account. I believe that that conversation further demonstrates that SCHEMER#1 was clearly keeping tabs on the schemers' activities at the banks, and doing so while present at SUBJECT PREMISES #1.

g. At approximately 4:35 p.m., I saw SCHEMER#1 exit building 10987 carrying a dark colored satchel (SUBJECT BAG #1). I followed SCHEMER#1 to the southeast exit of the Avalon Apartments complex. SCHEMER#1 exited the apartment complex with a fob key. I immediately notified SA Leonard, who was positioned on Bluffside Drive. SA Leonard told me that he saw SCHEMER#1 enter into an Acura MDX carrying his satchel. The Acura MDX had a California license plate of 7HUW657 (SUBJECT VEHICLE #1). SA Ou followed SCHEMER#1 to a Community Hospital in the city of Glendale, California. I researched license plate 7HUW657 in California Department of Motor Vehicle data base and learned that it was registered to SCHEMER#1.

257. December 3, 2015: On December 3, 2015, while conducting surveillance of SUBJECT PREMISES #1, I observed SCHEMER#8 in the passenger side of a black Range Rover. I recognized the driver of the Range Rover as SCHEMER#15, who as described above is a known runner of this scheme. I observed SCHEMER#15 park his vehicle across from building 10987 of the Avalon Apartments complex. Immediately after the vehicle was parked, SCHEMER#8 exited the vehicle and ran into building

10987. SCHEMER#8 emerged from the building a few minutes later and re-entered SCHEMER#15's black Range Rover. I followed SCHEMER#8 and SCHEMER#15 to a Wells Fargo Bank located in Encino, California, where I saw both of them enter the bank.

a. SCHEMER#8 and SCHEMER#15 remained in the bank for approximately 30 minutes before exiting and returning to the Avalon Apartments complex.

b. I was later told by a Wells Fargo fraud investigator that SCHEMER#8 and SCHEMER#15 had attempted to negotiate checks while inside the bank on December 3, 2015.

258. December 7, 2015: On December 7, 2015, SA Ou and I conducted a surveillance operation at the Avalon Apartment complex.

a. At approximately 10:30 a.m., we observed SCHEMER#8 sitting in a white 2014 Lexus ES 350. SA Ou and I observed SCHEMER#8 exit that vehicle and walk into the Avalon Apartments complex. After SCHEMER#8 walked into the apartment complex, I managed to record the Vehicle Identification Number ("VIN") from the dashboard of the 2014 Lexus ES 350. SA Ou researched that VIN and found that the 2014 Lexus ES 350 is registered to Jacqueline Nalbandyan and Migran Isakulyan, 10947 Huston St. #107, Toluca Lake, California 91602. Based on my training, experience, and conversations with other senior investigators, it is common for fraudsters or people who are committing crimes to drive vehicles not registered in their

names, in order to avoid being detected by law enforcement while continuing to engage in fraudulent activity.

b. At approximately 12:26 p.m., I was notified by Yolian that someone had called the bank, representing to be "Hrant Abovyan," and was inquiring about the status of his bank accounts. Yolian told the caller that Citibank had decided to close his bank accounts and that he would have to come into the branch to pick up the remaining balance in his accounts. "Hrant Abovyan" told Yolian that he would be in later that day to pick up his money.

c. Approximately 15 minutes later, at approximately 12:43 p.m., I saw SCHEMER#8 and SCHEMER#13 exit the Avalon Apartments complex together. In anticipation that they would be going to Yolian's Citibank's branch, SA Ou and I drove to that branch to set up surveillance.

d. At approximately 1:23 p.m., SA Ou and I observed SCHEMER#8 and SCHEMER#13 arrive at the Citibank in SCHEMER#8's Lexus. SCHEMER#13 was driving SCHEMER#8's vehicle and parked in front of the bank. SCHEMER#8 exited the Lexus and entered the bank alone.

e. At approximately 1:24 p.m., Yolian sent me a text informing me that the individual who had been posing in the identity of "Hrant Abovyan" had walked into her bank branch. Yolian told me that SCHEMER#8 again presented a Republic of Armenia passport in the name of "Hrant Abovyan." The passport displayed a photo of SCHEMER#8. Yolian told me that she closed

the bank accounts in the name of "Hrant Abovyan" and issued SCHEMER#8 a cashier's check for \$4,890.03, which was the remaining balance in those accounts.

f. At approximately 1:46 p.m., I observed SCHEMER#8 exit the bank holding a document in his hand and enter SCHEMER#8's Lexus in which he had arrived to the bank. SCHEMER#8 and SCHEMER#13 drove away. SA Ou and I attempted to follow them, however, we decided to discontinue our surveillance because we believe SCHEMER#13 was performing counter surveillance techniques. For example, we noticed SCHEMER#8 and SCHEMER#13 looking in their rear view mirror immediately after driving away from the bank. They were also driving down side streets at a slow speed.

g. At approximately 2:48 p.m., SA Ou and I returned to the Avalon Apartments complex and saw that SCHEMER#8's white 2014 Lexus ES 350 was now parked across from the Avalon Apartments complex.

h. On or about February 22, 2016, I received surveillance video, photographs, and bank records for an East West Bank account opening in the name of "Hrant Abovyan."

i. After reviewing monthly bank statements for that account, I discovered that the Citibank cashier's check in the amount of \$4,890.03 was deposited on December 7, 2015, the same day the cashier's check was given to SCHEMER#8. I also reviewed the video relating to this deposit, which shows SCHEMER#8 depositing the Citibank cashier's check at approximately 2:07

p.m. (As the paragraph above shows, SCHEMER#8 had received the Citibank cashier's check sometime between 1:24 and 1:46 p.m.) The deposit was made at the East West Bank Silver Lake branch located approximately 3 miles from the Citibank where SCHEMER#8 had been handed the cashier's check.

259. December 9, 2015:

a. On December 9, 2015, I interviewed Yolian. Yolian told me the following regarding her interactions with the individual posing as "Hrant Abovyan" (SCHEMER#8) on December 7, 2015:

i. She described SCHEMER#8 as a Russian Armenian who appeared to be 34-40 years old.

ii. SCHEMER#8 told Yolian that he intends on returning to Armenia within the month.

iii. Yolian examined the passport that SCHEMER#8 had provided and noticed that there was only one page that showed an entry into a country.

iv. Yolian recalls SCHEMER#8 laughing at the fact that his bank account was closed.

v. SCHEMER#8 gave Yolian his Citibank Debit Card prior to leaving the bank with his cashier's check.

b. Immediately following my interview with Yolian, I returned to the Avalon Apartments complex. At approximately 2:35 p.m., I was monitoring the balcony of SUBJECT PREMISES #1 from the Garland Hotel parking lot with my binoculars. During

this time, I saw SCHEMER#8 standing on the balcony of SUBJECT PREMISES #1.

260. December 23, 2015: On December 23, 2015, I was monitoring the entrance of building 10987 of the Avalon Apartments complex, while sitting in the Business Community Center there. At approximately 1:34 p.m., I observed SCHEMER#15 drive into the Avalon Apartments complex through the main entrance off of Vineland Avenue, driving the same black Range Rover with dealer license plates from "E3 Motors." SCHEMER#15 stopped in front of building 10987, and SCHEMER#14 exited the vehicle and ran into building 10987. SCHEMER#14 returned approximately three minutes later and re-entered the vehicle. SCHEMER#14's action of being dropped off, quickly running into Building 10987, entering SUBJECT PREMISES #1, and shortly thereafter returning to the vehicle, are consistent with runners who have been observed entering and quickly leaving the apartment complex where SUBJECT PREMISES #1 is located, to then proceed to visit banks as part of this fraudulent scheme.

261. January 6, 2016: On January 6, 2016, Citibank Branch Manager Yolian informed me that SCHEMER#6 and SCHEMER#5 had come into her branch, and SCHEMER#6 had identified herself as "Anahit Israyelyan." SCHEMER#6 had inquired why the funds in her bank accounts were frozen, and SCHEMER#6 and SCHEMER#5 were told that the accounts were under review. SCHEMER#6 and SCHEMER#5 implied that they would return the following day at 1:00 p.m. to speak with Yolian.

262. January 7, 2016:

a. On January 7, 2016, SA Ou, SA Leonard, and I conducted a surveillance operation at the Citibank branch located at 1900 W. Sunset Blvd., Los Angeles, California (the same branch at which SCHEMER#8 had previously met with bank employee Yolian regarding the bank account opened in the name of "Hrant Abovyan").

b. At approximately 12:58 p.m., I saw SCHEMER#5 drive into the Citibank parking lot in a black 2016 Lexus SUV with black dealer plates that read "Maya Motors."

c. At approximately 1:00 p.m., Yolian notified me that SCHEMER#6 and SCHEMER#5 had entered the bank together. Yolian sat with /SCHEMER#6 and SCHEMER#5 to discuss the bank account in the name of "Anahit Israyelyan."

d. At approximately 1:10 p.m., Yolian informed me that of "Anahit Israyelyan" and a Citibank Debit card in the name of "Anahit Israyelyan." The passport displayed a picture of SCHEMER#6. Yolian photocopied the passport and texted me a copy. After viewing the passport photo, I confirmed the woman in bank was in fact the individual I knew as SCHEMER#6.

e. Yolian told me that her conversation with SCHEMER#6 and SCHEMER#5 were in Armenian. SCHEMER#6 claimed that she had opened the bank account on behalf of her son. In fact, SCHEMER#6 stated that Yolian had previously helped her son on his own account; however, when asked what the name of her son was, SCHEMER#6 initially could not recall. SCHEMER#6 also

represented to Yolian that she had several businesses in Armenia and had lots of money; however, she again could not name even one of her purported businesses. When asked for her address and phone number, SCHEMER#6 stated that she did not know. Yolian told SCHEMER#6 and SCHEMER#5 that Citibank froze the "Anahit Israyelyan" bank accounts because the checks deposited into her account were flagged as fraudulent. Yolian told SCHEMER#6 that her account is under review and that the bank would notify her once a decision has been made. SCHEMER#6 told Yolian that her phone number and address information is in the car and that she would call Yolian to provide this information.

f. At approximately 1:22 p.m., Yolian notified me that SCHEMER#5 and SCHEMER#6 had exited the bank.

g. At approximately 1:30 p.m., I drove into the Citibank parking lot. During this time I saw SCHEMER#5 sitting in the driver side of the black Lexus SUV talking on her cell phone and SCHEMER#6 was sitting in the passenger side.

h. At approximately 1:32 p.m., SCHEMER#5 and SCHEMER#6 departed by vehicle. SA Ou, SA Leonard, and I followed SCHEMER#5 and SCHEMER#6 to the Avalon Apartments complex. SCHEMER#5 drove down the guest drive way which leads to the south east entrance/exit of the apartment complex. SA Leonard was on foot maintaining visual observation. SA Leonard told me that he saw SCHEMER#5 and SCHEMER#6 waiting in the vehicle for approximately ten minutes. During this time,

SCHEMER#5 honked the vehicle's horn as if she were waiting for someone.

i. At approximately 1:55 p.m., SA Leonard informed me that SCHEMER#5 was driving away and proceeding towards Vineland Ave. SA Ou and I were parked in front of the Avalon Apartments complex main entrance on Vineland Ave. I saw SCHEMER#5 drive a few feet passed the Avalon Apartments complex entrance, where she pulled over and parked. Immediately after parking, an unknown female adult wearing black clothing exited the rear passenger side of SCHEMER#5's vehicle and ran back into the Avalon Apartments complex. The woman I saw exiting SCHEMER#5's vehicle matched the description of the unknown woman I saw on the balcony of SUBJECT PREMISES #1 on previous dates.

j. SCHEMER#5 continued to drive north on Vineland Ave. before being pulled over by Los Angeles Police Officers Godoy and Mitchell. SCHEMER#5 was stopped for not having a license plate. Officers Godoy later told SA Ou who informed me that SCHEMER#5 identified herself as the registered owner of the vehicle. She provided a California driver's license displaying her photo, name, and address. Officers Godoy stated that SCHEMER#5 had on blue contact lenses and was potentially wearing a black wig. The police officers confirmed that the vehicle was registered to SCHEMER#5. The police officers released SCHEMER#5 without citing her. As the police officers were walking away, they heard laughing coming from the vehicle.

k. After being questioned by the police, SCHEMER#5 and SCHEMER#6 were followed to the East West Bank located 135 N. Robles Ave., Pasadena, California. At approximately 2:45 p.m., I saw both SCHEMER#5 and SCHEMER#6 enter the bank together.

l. At approximately 3:00 p.m., SCHEMER#5 and SCHEMER#6 exited the bank and entered their vehicle. SCHEMER#5 and SCHEMER#6 were then followed to the Wells Fargo Bank located at 82 S. Lake Ave., Pasadena, California, a few miles from East West Bank. SA Leonard told me that he saw SCHEMER#5 and SCHEMER#6 enter the bank and approach a Wells Fargo team member. At approximately 3:18 p.m., I walked inside the Wells Fargo Bank and saw SCHEMER#5 and SCHEMER#6 sitting with a Wells Fargo team member at a private cubicle.

m. About a half hour later, at approximately 3:30 p.m., I observed SCHEMER#5 and SCHEMER#6 drive away from the Wells Fargo Bank. We followed them from that bank to the city of Glendale, where SCHEMER#5 dropped off SCHEMER#6 in the Jon's Supermarket parking lot located on Colorado Blvd. We discontinued surveillance of SCHEMER#5, because we had confirmed her identity earlier in the day. SA Ou, SA Leonard, and I maintained surveillance of SCHEMER#6 in hopes that we would be able to determine where she resides. SCHEMER#6 was then picked up by an unknown female who was driving a newer Jeep Cherokee with dealer license plate. We followed the vehicle to an apartment complex located at 208 W. Maple Ave., Glendale,

California. Because we were unable to identify the apartment in which SCHEMER#6 entered, her identity remains unknown.

263. January 8, 2016:

a. On January 8, 2016, SA Ou and I interviewed Jessy Yang ("Yang") and Clayton Tso ("Tso"), East West Bank team members who work at the branch located at 135 N. Los Robles Ave., Pasadena, California. Yang told me that she recalled assisting SCHEMER#6 and SCHEMER#5 on the previous day.

SCHEMER#6 claimed that she did not speak English. SCHEMER#5 then translated the conversation between SCHEMER#6 and Yang in English.

b. Yang stated that SCHEMER#6 identified herself as "Elena Oganessian" and provided a passport from the country of Georgia containing her photograph. Yang examined the passport presented by SCHEMER#6, and recalled that the photograph on the passport appeared to be simply glued on. The purpose of SCHEMER#6's visit was to provide a change of address, a check book, and a new debit card. However, it was SCHEMER#5 who provided Yang with SCHEMER#6's new address. Yang told me that she believes Jane Doe and SCHEMER#5 were wearing wigs and hair extensions. I presented Yang with a copy of the Republic of Armenia passport that SCHEMER#6 had presented to Citibank Manager Yolian a few hours before, which was in the name of "Anahit Israyelyan." Yang reviewed the photograph and confirmed the person in the "Anahit Israyelyan" passport from the Republic

of Armenia was the same woman who had identified herself as "Elena Oganesyra" with a passport from the country of Georgia.

c. I also showed the same copy of the "Anahit Israyelyan" passport to Tso. He reviewed the passport photograph and told me that he recognized the woman in the photo to be the same woman he had assisted in opening an account in August 2015. However, Tso recalls that the person in the passport photograph had identified herself as "Elena Oganesyran." Tso stated that SCHEMER#6 opened the "Elena Oganesyran" account with a country of Georgia passport bearing SCHEMER#6's photograph.

d. East West Bank provided me with SCHEMER#6's updated address. According to the signature card for "Elena Oganesyran," she indicated to East West Bank at the time she opened her bank accounts that she resided at 1107 Fair Oaks Ave., Pasadena, California 91303. However, she now wished to change her address to 1107 Fair Oaks Ave., Apt. 859, Pasadena, California 91303.

e. Immediately following our interview with Yang and Tso, SA Ou and I drove by the address 1107 Fair Oaks Ave., Apt. 859, Pasadena, California 91303. We discovered that 1107 Fair Oaks Ave., Apt. 859, Pasadena, California 91303, was actually not an apartment, but rather, was a UPS Store. So, SA Ou and I interviewed the UPS Store owner there. The UPS Store owner confirmed that a private mailbox was being rented by "Elena Oganesyran;" however, she was renting mailbox #858 and not #859.

I was provided with the mailbox Service Agreement, U.S. Postal Service Application for Delivery of Mail Through Agent (Form 1583), a Time Warner Cable Bill, a Georgian Passport, and Costco Membership Card in the name of "Elena Oganessian" that were used to rent the mailbox. The Georgian passport and Costco card depicted a photo of SCHEMER#6.

264. January 12, 2016:

a. On January 12, 2016, I was monitoring the balcony of SUBJECT PREMISES #1 live via a pole camera. During this time, I witnessed SCHEMER#1, SCHEMER#13, UF1, SCHEMER#14, SCHEMER#15, and an unknown adult male on the balcony of SUBJECT PREMISES #1.

b. At approximately 4:45 p.m., I saw SCHEMER#14 show what appear to be several white colored documents to the unknown male.

265. January 14, 2016: On January 14, 2016, I was monitoring the GPS tracker on the white 2014 Lexus ES 350 driven by SCHEMER#8.

a. At approximately 12:30 p.m., the GPS tracker indicated that the vehicle was parked at the Avalon Apartments complex.

b. At approximately 3:02 p.m., the GPS tracker showed that the vehicle was now parked across the street from Wells Fargo Bank located at 12900 Ventura Blvd., Studio City, California.

c. The GPS tracker indicated that at approximately 3:40 p.m., the vehicle had begun to travel back from the bank towards the Avalon Apartments complex.

d. According to the GPS tracker, the vehicle was parked across the street from Avalon Apartments complex at approximately 3:45 p.m.

266. January 22, 2016:

a. On January 22, 2016, I interviewed Citibank Manager Yolian after she informed me that SCHEMER#6 and an unknown male (subsequently identified as SCHEMER#15) who drove a black Range Rover with yellow dealer plates had been in her bank inquiring about the account SCHEMER#6 had opened under the name "Anahit Israyelyan." Yolian told me that SCHEMER#6 and the unknown male visited the Citibank branch in Korea Town earlier in the day asking to have her account unfrozen. Yolian told me that the unknown male represented himself as a friend of SCHEMER#6's son. Yolian told me that she explained to SCHEMER#6 and the unknown male that SCHEMER#6's "Anahit Israyelyan" bank account was frozen because a review of her account revealed that she deposited checks from individuals who had received fraudulent tax refunds. According to Yolian, the unknown male turned to SCHEMER#6 and said in Armenian, "They screwed you." SCHEMER#6 replied to Yolian saying that she could not believe what was going on because the money in her account was hers. However, Yolian told me that SCHEMER#6 did not appear to be surprised when she was told that the funds would not be made

available to her. Yolian was shown a photograph of SCHEMER#15 standing on the balcony of SUBJECT PREMISES #1 on January 12, 2016. Yolian identified the person in that photograph as the same person who had accompanied SCHEMER#6 in the bank and who was driving the black Range Rover.

b. After my interview with Yolian, I drove to the Avalon Apartments complex to see if I could identify the black Range Rover. At approximately 4:24 p.m., I arrived at the Avalon Apartments complex. As I was parking my vehicle, I saw SCHEMER#1 walk into the Avalon Apartments complex carrying a dark colored satchel or laptop bag (SUBJECT BAG #1). SCHEMER#1 entered the Avalon Apartments complex with a fob key. I followed SCHEMER#1 and confirmed that he entered building 10987, which is the building that houses SUBJECT PREMISES #1.

c. At approximately 4:52 p.m., approximately thirty minutes later, SA Leonard notified me that he observed SCHEMER#1 standing on the balcony of SUBJECT PREMISES #1. At that time, I was positioned inside the Avalon Apartment Business Center located across from building 10987. I was also monitoring the pole camera from my laptop computer.

d. At approximately 5:00 p.m., I observed a black Range Rover with yellow dealer license plate drive into the Avalon Apartments complex. The Range Rover drove to the underground parking structure of building 10987.

e. At approximately 5:03 p.m., I saw SCHEMER#13 and SCHEMER#9 talking to each other on the balcony of SUBJECT PREMISES #1.

f. At approximately 5:04 p.m., I saw SCHEMER#8 exit building 10987. It appeared that SCHEMER#8 had a white envelope or document in his rear pants pocket.

g. At approximately 6:55 p.m., I observed SCHEMER#1 and the unknown female exit SUBJECT PREMISES #1 together. SCHEMER#1 was carrying the same dark colored satchel (SUBJECT BAG #1) seen earlier in the day, which had also been observed on many prior occasions. I followed SCHEMER#1 to his vehicle, an Acura MDX with license plate 7HUW657 (SUBJECT VEHICLE #1). I then observed SCHEMER#1 place SUBJECT BAG #1 into SUBJECT VEHICLE #1 and drive away. I attempted to follow SCHEMER#1; however, I was unable to maintain surveillance. SCHEMER#1 was last seen driving northbound on the 101 North Freeway towards the direction of his residence.

267. January 27, 2016:

a. On January 27, 2016, I followed SCHEMER#8 from his residence to an apartment complex located on North Adams Street, in Glendale, California.

b. At approximately 11:49 a.m., I saw SCHEMER#8 and SCHEMER#9 walk from one of the apartment buildings and enter SCHEMER#8's vehicle.

c. I followed them to a second residence located a few miles away, where I observed SCHEMER#8, SCHEMER#9, and

another unknown male adult have a conversation with each other on the side of the road. After talking for an approximately ten minutes, all three individuals entered SCHEMER#8's vehicle and drove away.

d. I followed the individuals to the Avalon Apartments complex. SCHEMER#8 parked his vehicle on Bluffside Drive, across from the Avalon Apartments complex. As I was walking towards SCHEMER#8's vehicle, I saw that SCHEMER#1's Acura MDX was also parked on Bluffside Drive.

e. At approximately 12:49 p.m., I walked down to the underground parking structure of building 10987 and saw SCHEMER#15's black Range Rover parked in parking space #25. Based on my conversations with Avalon Apartments complex management personnel, I know that space #25 is assigned to SUBJECT PREMISES #1. The Range Rover had yellow McKenna dealer plates; however, the vehicle had an E3 Motors sales and leasing registration sticker on the lower part of the front windshield. I believe SCHEMER#15 switched his dealer plates to avoid being detected from law enforcement while driving Tier-2 bank account holders to and from banks. I researched the VIN of the black Range Rover and found that it is registered to Ashot Hakverdyan and Razmik Hakverdyan. California Department of Motor Vehicle data base also confirmed that the Range Rover has been assigned license plate number 6FTE706.

f. At approximately 1:19 p.m., SA Leonard notified me that he was monitoring the pole camera and saw SCHEMER#8 and SCHEMER#1 standing on the balcony of SUBJECT PREMISES #1.

g. At approximately 1:30 p.m., Yolian notified me that a man claiming to be the son of "Anahit Israyelyan" had just called inquiring about the "Anahit Israyelyan" bank account.

h. At approximately 1:38 p.m., I saw SCHEMER#15 and an unknown male adult, who was wearing a white and black sweater, walk out of SUBJECT PREMISES #1. Approximately three minutes later, I saw the black Range Rover with yellow McKenna dealer plates drive out from the underground parking lot and out of the apartment complex.

i. At approximately 1:53 p.m., SA Leonard emailed me a photograph of SCHEMER#1, SCHEMER#8, and SCHEMER#13 together on the balcony of SUBJECT PREMISES #1.

j. At approximately 2:02 p.m., I was monitoring the pole camera from the Avalon Apartments complex Business Center from my laptop when I saw SCHEMER#9 standing on the balcony of SUBJECT PREMISES #1 and talking to SCHEMER#13.

k. At approximately 2:55 p.m., I observed SCHEMER#8 walk out of building 10987 towards his vehicle on Bluffside Drive. As SCHEMER#8 was walking to his vehicle, SCHEMER#12 drove into the Avalon Apartments complex. The two individuals had a brief conversation with each other. SCHEMER#12, however, continued on and drove towards the underground parking structure

of building 10987. At approximately 3:05 p.m., I saw SCHEMER#12 drive out from the underground parking structure of building 10987 and out of the apartment complex.

l. According to the GPS tracker, at approximately 3:10 p.m., SCHEMER#8 stopped at the Mailbox Plus shipping and mail center, located at 5404 Whitsett Ave., Valley Village, California. After interviewing the manager of Mailbox Plus, SA Ou later confirmed that SCHEMER#8 had picked up mail from a mailbox there.

m. At approximately 3:15 p.m., I left the Avalon Business Center to locate SCHEMER#8. At approximately 3:40 p.m., the GPS tracker showed that SCHEMER#8's vehicle had parked in front of Mail Call, a mailbox center located at 5870 Melrose Ave., Los Angeles, California. The GPS tracker indicated that the vehicle had departed at approximately 3:45 p.m. I then interviewed the owner of Mail Call who told me that SCHEMER#8 had just left. He stated that SCHEMER#8 had wanted to open a mailbox with only one form of secondary identification - a Time Warner Cable Bill. The owner said that SCHEMER#8 had a passport that was burgundy in color, but that he told SCHEMER#8 that he also needed to provide a second form of identification. The owner said upon hearing that response, SCHEMER#8 walked out.

n. At approximately 4:05 p.m., I then followed SCHEMER#8 to Sunset Boulevard Mailboxes located at 7119 La Brea Blvd., Los Angeles, California. As I was driving into the parking lot there, I saw SCHEMER#8 pulling out of a parking

spot. I waited until SCHEMER#8 drove away before interviewing John Park ("Park"), the owner of Sunset Boulevard Mailboxes. I showed a photo of SCHEMER#8 to Park who recognized SCHEMER#8 and stated that he had just been in, asking to rent a mailbox for three months. Park said that he told SCHEMER#8 that he only rents mailboxes for a period of one year. Park said SCHEMER#8 left after hearing this information.

o. After my interview with Park, I located SCHEMER#8's vehicle on Ogden Drive, across the street from the Bank of America located at 7800 W. Sunset Blvd., Los Angeles, California. At approximately 4:34 p.m., I saw SCHEMER#8 and SCHEMER#13 walk away from the Bank of America. They then entered SCHEMER#8's vehicle and continued west on Sunset Blvd.

p. After SCHEMER#8's vehicle departed that location, I continued to follow SCHEMER#8 as he drove westbound on Sunset Blvd. At approximately 4:41 p.m., SCHEMER#8 arrived at Boxes and More, a mail center located at 8491 Sunset Blvd, West Hollywood, California. SCHEMER#8 remained in Boxes and More for approximately five minutes before leaving and driving back to the Bank of America. After SCHEMER#8 drove away from Boxes and More, I interviewed Pablo, who identified himself to me as the owner of Boxes and More. I showed Pablo a photograph of SCHEMER#8. After seeing the photograph of SCHEMER#8, Pablo stated that SCHEMER#8 had just rented a mailbox under the name of "Edik Nasirov." Pablo provided me with a photocopy of a Georgia Passport that had a photo of SCHEMER#8 on it. Pablo

said that SCHEMER#8 signed a United States Postal Service Application for Delivery of Mail Through Agent, Form 1583, under the name "Edik Nasirov." Pablo provided me with a copy of the Form 1583 signed by SCHEMER#8 using the name "Edik Nasirov," which was dated January 27, 2016.

q. After my interview with the owner of Boxes and More, I resumed tracking SCHEMER#8. The GPS tracker indicated that his vehicle was parked across the street from the same Bank of America located at 7800 Sunset Blvd, Los Angeles, California. While in route to the Bank of America from Boxes and More, I called a Bank of America fraud investigator and notified the investigator of a potential fraud in progress. The bank investigator told me that the investigator would call the branch and inquire if someone had recently opened a bank account using a foreign passport or a passport from the country of Georgia. The bank investigator returned my call and told me that the branch manager confirmed that sometime between 4:30 p.m. and 5:30 p.m., a business bank account had been opened under the name "Lotex." He said that the account owner opened the account using a passport from the country of Georgia, and that the account owner identified himself as "Nugzar Arutinov." "Nugzar Arutinov" also presented a Time Warner Cable Bill. The bank investigator also stated that "Nugzar Arutinov" made an initial deposit of \$300 through the branch ATM machine outside. According to the Bank Manager, "Nugzar Arutinov" claimed to be a furniture manufacturer.

r. At approximately 5:21 p.m., SCHEMER#8's vehicle left Bank of America and drove back to the Avalon Apartments complex. At approximately 6:17 p.m., I arrived at the Avalon Apartments complex and continued my surveillance on foot. I walked down to the underground parking structure of building 10987 and saw SCHEMER#8's vehicle parked in the assigned parking spot #25, which is the spot for SUBJECT PREMISES #1.

268. As discussed above under the section discussing SCHEMER#15, I believe SCHEMER#15 and the other fraudsters who frequent SUBJECT PREMISES #1 are also involved in account takeover schemes and use SUBJECT PREMISES #1 to safe keep checks related to those other fraudulent schemes (such as involving fictitious checks or account takeovers) they are also orchestrating.

269. January 28, 2016:

a. On January 28, 2016, at approximately 4:49 p.m., a bank investigator emailed me a photograph of the individual posing as "Nugzar Arutinov" making his \$300 initial deposit at the ATM machine. The photograph was date-stamped January 27, 2016, at 5:12 p.m. After reviewing the photograph of "Nugzar Arutinov," I recognized the person to be SCHEMER#9. In fact, I recognized the jacket he was wearing in the photograph as the same jacket I had seen him wear earlier that day. The bank investigator also stated that "Nugzar Arutinov" provided an address of 5404 Whitsett Ave., Valley Village, California. I

know based on my surveillance of SCHEMER#8 the previous day that this address is where Mailbox Plus is located.

b. On January 28, 2016, HSI SA Ou interviewed the manager at Mailbox Plus located at 5404 Whitsett Ave., Valley Village, California. SA Ou told me the following regarding his interview and the records that he was provided. SA Ou inquired if any mailboxes were rented in the name of "Nugzar Arutinov." SA Ou was provided with a United States Postal Service Application for Delivery of Mail Through Agent, Form 1583, for mailbox #179 leased in the name of "Nugzar Arutinov." SA Ou was also provided with a country of Georgia Passport that displayed a purported photograph of "Nugzar Arutinov" and a Time Warner Cable Bill that "Nugzar Arutinov" had provided as a second form of identification. SA Ou provided these documents to me for my review. After viewing the photograph displayed on the Georgia Passport in the name of "Nugzar Arutinov," I recognized the person to be the same person in the Bank of America ATM surveillance photo and that of John Doe/SCHEMER#9. According to the Form 1583, SCHEMER#9 opened mailbox #179 on or about January 8, 2016.

270. February 2016: In or around February 2016, SA Ou spoke with the leasing manager of the Avalon Apartments complex. The leasing manager told SA Ou that in February 2016, he had conducted an inspection of SUBJECT PREMISES #1 and other apartments in building 10987, due to renovation plans. The leasing manager told SA Ou, who subsequently told me, that he

saw a desktop computer inside SUBJECT PREMISES #1 during the inspection on February 2016.

271. February 3, 2016:

a. On February 3, 2016, I was monitoring the GPS tracker on SCHEMER#8's vehicle and the pole camera directed at the balcony of SUBJECT PREMISES #1. At approximately 2:15 p.m., the GPS tracker indicated that SCHEMER#8's vehicle was parked across the street from the Avalon Apartments complex. The GPS tracking history also indicated that SCHEMER#8's vehicle had stopped on N. Adams Street, Glendale, California, which is the location I had seen SCHEMER#8 and SCHEMER#9 come from on January 27, 2016. The tracking history also showed that SCHEMER#8's vehicle stopped on the corner of Doran Ave. and Pacific Ave. in Glendale, California. This is the exact location where I saw SCHEMER#8, SCHEMER#9, and an unknown male enter SCHEMER#8's vehicle and drive to the Avalon Apartments complex.

b. At approximately 3:05 p.m., I saw SCHEMER#1, SCHEMER#9, and SCHEMER#8, standing on the balcony of SUBJECT PREMISES #1 talking to each other.

272. February 4, 2016:

a. On February 4, 2016, from my laptop, I was monitoring SCHEMER#8's movement from the GPS tracker. At the time, I was in the Avalon Apartments complex Business Center.

b. At approximately 11:00 a.m., the GPS tracker showed SCHEMER#8's vehicle parked on N. Adams St., Glendale, California. Based on SCHEMER#8's driving patterns, I believe